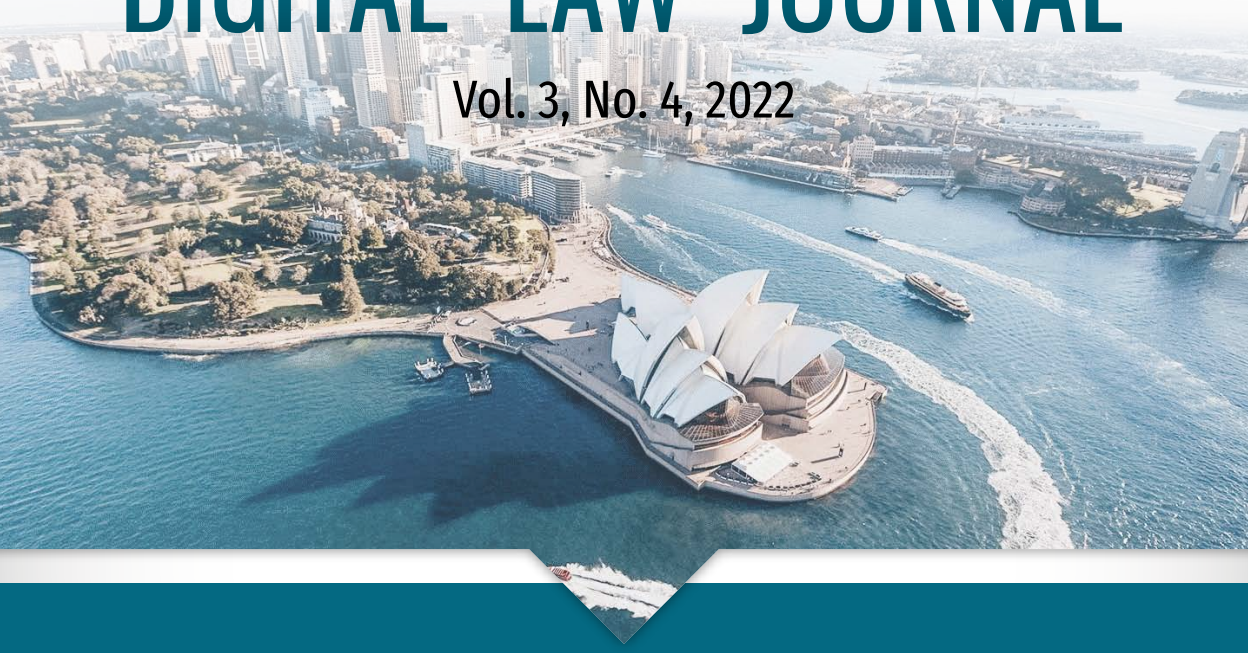
ISSN 2686-9136 (Online)

DIGITAL LAW JOURNAL

Vol. 3, No. 4, 2022



ESSAYS

ARTICLES

BOOK REVIEW

DIGITAL LAW JOURNAL

DIGITAL LAW JOURNAL

Journal of research and practice

Published since 2020
4 issues per year

Vol. 3, No. 4, 2022

ЦИФРОВОЕ ПРАВО

Научно-практический журнал

Журнал издается с 2020 г.
4 выпуска в год

Том 3, № 4, 2022

Contents

Essays

Articles

Book Review

Содержание

Эссе

Статьи

Рецензия на книгу

DIGITAL LAW JOURNAL

AIMS AND SCOPE

The purpose of the Digital Law Journal is to provide a theoretical understanding of the laws that arise in Law and Economics in the digital environment, as well as to create a platform for finding the most suitable version of their legal regulation. This aim is especially vital for the Russian legal community, following the development of the digital economy in our country. The rest of the world has faced the same challenge, more or less successfully; an extensive practice of digital economy regulation has been developed, which provides good material for conducting comparative research on this issue. Theoretically, "Digital Law" is based on "Internet Law", formed in English-language scientific literature, which a number of researchers consider as a separate branch of Law.

The journal establishes the following objectives:

- Publication of research in the field of digital law and digital economy in order to intensify international scientific interaction and cooperation within the scientific community of experts.
- Meeting the information needs of professional specialists, government officials, representatives of public associations, and other citizens and organizations; this concerns assessment (scientific and legal) of modern approaches to the legal regulation of the digital economy.
- Dissemination of the achievements of current legal and economic science, and the improvement of professional relationships and scientific cooperative interaction between researchers and research groups in both Russia and foreign countries.

The journal publishes manuscripts in the following fields of developments and challenges facing legal regulation of the digital economy:

1. Legal provision of information security and the formation of a unified digital environment of trust (identification of subjects in the digital space, legally significant information exchange, etc.).
2. Regulatory support for electronic civil turnover; comprehensive legal research of data in the context of digital technology development, including personal data, public data, and "Big Data".
3. Legal support for data collection, storage, and processing.
4. Regulatory support for the introduction and use of innovative technologies in the financial market (cryptocurrencies, blockchain, etc.).
5. Regulatory incentives for the improvement of the digital economy; legal regulation of contractual relations arising in connection with the development of digital technologies; network contracts (smart contracts); legal regulation of E-Commerce.
6. The formation of legal conditions in the field of legal proceedings and notaries according to the development of the digital economy.
7. Legal provision of digital interaction between the private sector and the state; a definition of the "digital objects" of taxation and legal regime development for the taxation of business activities in the field of digital technologies; a digital budget; a comprehensive study of the legal conditions for using the results of intellectual activity in the digital economy; and digital economy and antitrust regulation.
8. Legal regulation of the digital economy in the context of integration processes.
9. Comprehensive research of legal and ethical aspects related to the development and application of artificial intelligence and robotics systems.
10. Changing approaches to training and retraining of legal personnel in the context of digital technology development; new requirements for the skills of lawyers.

The subject of the journal corresponds to the group of specialties Legal Sciences 5.1.0. and Economic Sciences 5.2.0. according to the HAC nomenclature.

The journal publishes manuscripts in Russian and English.

FOUNDER, PUBLISHER:

Maxim I. Inozemtsev
76, ave. Vernadsky, Moscow, Russia, 119454

Founded:	The journal has been published since 2020
Frequency:	4 issues per year
DOI Prefix:	10.38044
ISSN online:	2686-9136
Mass Media Registration Certificate:	ЭЛ № ФС 77-76948 of 9 Oct. 2019 (Roskomnadzor)
Distribution:	Content is distributed under Creative Commons Attribution 4.0 License
Editorial Office:	76, ave. Vernadsky, Moscow, Russia, 119454, +7 (495) 229-41-78, digitallawjornal.org, dlj@digitallawjournal.org
Published online:	31 Dec. 2022
Copyright:	© Digital Law Journal, 2022
Price:	Free

REGION GROUP OF COMPANIES With support of REGION Group of Companies

ЦИФРОВОЕ ПРАВО

ЦЕЛИ И ЗАДАЧИ

Цель электронного журнала «Цифровое право» (Digital Law Journal) — создание дискуссионной площадки для осмысления в научно-практической плоскости легализации цифровых технологий, особенностей и перспектив их внедрения в нормативно-правовое поле. Особенно остро эта задача стоит перед российским сообществом правоведов в связи с развитием цифровой экономики в нашей стране. С этой же задачей сталкивается и остальной мир, решая её более или менее успешно. В мире сформировалась обширная практика нормативного регулирования цифровой экономики, она даёт хороший материал для проведения сравнительных исследований по этой проблематике. В теоретическом плане цифровое право опирается на сформировавшееся в англоязычной научной литературе академическое направление «интернет-право», которое ряд исследователей рассматривают как отдельную отрасль права.

Задачами журнала являются:

- Публикация исследований в области цифрового права и цифровой экономики с целью интенсификации международного научного взаимодействия и сотрудничества в рамках научного сообщества экспертов.
- Удовлетворение информационных потребностей специалистов-профессионалов, должностных лиц органов государственной власти, представителей общественных объединений, иных граждан и организаций в научно-правовой оценке современных подходов к правовому регулированию цифровой экономики.
- Распространение достижений актуальной юридической и экономической мысли, развитие профессиональных связей и научного кооперативного взаимодействия между исследователями и исследовательскими группами России и зарубежных государств.

В журнале публикуются рукописи по следующим направлениям развития и задачам, стоящим перед нормативным регулированием цифровой экономики.

1. Нормативное обеспечение информационной безопасности, формирование единой цифровой среды доверия (идентификация субъектов в цифровом пространстве, обмен юридически значимой информацией между ними и т. д.).
2. Нормативное обеспечение электронного гражданского оборота; комплексные правовые исследования оборота данных в условиях развития цифровых технологий, в том числе персональных данных, общедоступных данных, Big Data.
3. Нормативное обеспечение условий для сбора, хранения и обработки данных.
4. Нормативное обеспечение внедрения и использования инновационных технологий на финансовом рынке (криптовалюты, блокчейн и др.).
5. Нормативное стимулирование развития цифровой экономики; правовое регулирование договорных отношений, возникающих в связи с развитием цифровых технологий. Сетевые договоры (смарт-контракты). Правовое регулирование электронной торговли.
6. Формирование правовых условий в сфере судопроизводства и нотариата в связи с развитием цифровой экономики.
7. Обеспечение нормативного регулирования цифрового взаимодействия предпринимательского сообщества и государства; определение «цифровых объектов» налогов и разработка правового режима налогообложения предпринимательской деятельности в сфере цифровых технологий. Цифровой бюджет; комплексное исследование правовых условий использования результатов интеллектуальной деятельности в условиях цифровой экономики. Цифровая экономика и антимонопольное регулирование.
8. Нормативное регулирование цифровой экономикой в контексте интеграционных процессов.
9. Комплексные исследования правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта и робототехники.
10. Изменение подходов к подготовке и переподготовке юридических кадров в условиях развития цифровых технологий. Новые требования к навыкам и квалификации юристов.

Тематика журнала соответствует группе специальностей «Юридические науки» 5.1.0 и «Экономические науки» 5.2.0 по номенклатуре ВАК.

В журнале публикуются рукописи на русском и английском языках.

УЧРЕДИТЕЛЬ, ИЗДАТЕЛЬ:

Иноземцев Максим Игоревич
119454, Россия, Москва, просп. Вернадского, 76

История издания журнала:	Журнал издается с 2020 г.
Периодичность:	4 выпуска в год
Префикс DOI:	10.38044
ISSN online:	2686-9136
Свидетельство о регистрации средства массовой информации:	№ ФС 77-76948 от 09.10.2019 (Роскомнадзор)
Условия распространения материалов:	Контент доступен под лицензией Creative Commons Attribution 4.0 License
Редакция:	119454, Россия, Москва, просп. Вернадского, 76, +7 (495) 229-41-78, digitallawjournal.org, dlj@digitallawjournal.org
Дата публикации:	31.12.2022
Копирайт:	© Цифровое право, 2022
Цена:	Свободная

РЕГИОН ГРУППА КОМПАНИЙ При поддержке Группы компаний «РЕГИОН»

https://doi.org/10.38044/2686-9136-2022-3-4-8-31

ESSAYS

VIDEO GAME MODDING IN THE U.S. INTELLECTUAL PROPERTY LAW: CONTROVERSIAL ISSUES AND GAPS

Christie A. Lee

University of California
200 McAllister St., San Francisco, California, United States of America, CA 94102

Abstract

This essay's purpose is to illustrate a broad understanding of legal issues and gaps in U.S. law regarding video game modifications. Digital entertainment technology develops so quickly that often new technology does not fit precisely into current law and statutes. Two different approaches to video game modification are explored pertinent to companies' different attitudes toward modification by third parties and end-users. These two approaches include companies that encourage third party modifications, and companies that want to deter against third party modifications. Then, issues and risks of modification are explored through potential breach of contract, copyright infringement, and reverse engineering. The author analyzes the relevant court rulings on the matter of distributing these risks. Besides there are different forms of affirmative defenses such as fair use in the U.S case law which are also discussed in the article. Finally, gaps in the law and ownership issues regarding modifications are shown in the cases involving Blizzard Entertainment Inc. This essay is meant to illuminate the dichotomy of laws and courts protecting the interests of copyright holders, giving them protection and incentive to continue creating, versus anti-monopolistic rules, and providing the ultimate beneficiaries of video games the right to modify them.

Keywords

intellectual property law, USA, IP, video game, modding, IP remedies, copyright infringement, license agreement

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Lee, C. A. (2022). Video game modding in the U.S. intellectual property law: Controversial issues and gaps. *Digital Law Journal, 3*(4), 8–31. https://doi.org/10.38044/2686-9136-2022-3-4-8-31

Submitted: 3 June. 2022, accepted: 3 Oct. 2022, published: 31 Dec. 2022

ЭССЕ

ПРОБЛЕМЫ МОДИФИКАЦИИ ВИДЕОИГР В ПРАВЕ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ США

К.А. Ли

Калифорнийский университет
CA 94102, Соединенные Штаты Америки, Калифорния,
Сан-Франциско, ул. МакАллистер, 200

Аннотация

Цель данного эссе — проиллюстрировать широту юридических вопросов и пробелов в праве США, касающихся модификаций видеоигр. Цифровые развлекательные технологии развиваются так быстро, что зачастую они не укладываются в рамки действующего правового регулирования. В статье анализируются два различных подхода к модификации видеоигр, соответствующих разному отношению компаний к изменению их продукта третьими лицами и конечными пользователями: от поощрения до воздержания от использования сторонних модификаций. Правовые проблемы и риски, связанные с модификацией видеоигр, исследуются в нескольких плоскостях: с точки зрения потенциального нарушения договорного обязательства (*breach of contract*), с позиции нарушения авторских прав и в связи с разработкой программного обеспечения на основе копирования технологии, лежащей в основе видеоигры (*reverse engineering*). Автор рассматривает судебные решения по вопросу распределения данных рисков между сторонами. Также анализируются решения, вынесенными в пользу конечных пользователей, в частности на основе доктрины добросовестного использования (*fair use*). Наконец, автором продемонстрированы пробелы в интеллектуальном праве США на примере дел, в которых одной из сторон выступает компания *Blizzard Entertainment Inc.* Автор демонстрирует существующую в США двойственность подхода к защите прав на продукты игровой индустрии: с одной стороны, приоритет отдается охране интересов правообладателей и их стимулов для продолжения создания новых видеоигр, а с другой стороны, предпочтением пользуется интерес конечных бенефициаров, что дает право пользователям изменять игру согласно своим предпочтениям и выступать против монополизма компаний-разработчиков.

Ключевые слова

право интеллектуальной собственности, США, IP, видеоигры, модификация, средства защиты интеллектуальных прав, нарушение авторских прав, лицензионные соглашения

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.

Для цитирования Ли, К. А. (2022). Проблемы модификации видеоигр в праве интеллектуальной собственности США. *Цифровое право, 3*(4), 8–31. https://doi.org/10.38044/2686-9136-2022-3-4-8-31

Поступила: 03.06.2022, принята в печать: 03.10.2022, опубликована: 31.12.2022

Introduction

This essay begins with a legal definition of video game modification, as well as a brief overview of the copyright statute, (Copyright Act 1976, U.S.C. 17), which is the overarching law that presides over this area.

Then the examples of video game modifications and their creators are considered. Videogame modifications can be aesthetic, for example the change in the way something looks in a game. They can be functional, such as minor fixes utilized to make a game run properly or more smoothly. Finally, they can involve changing a game so completely that it is unrecognizable from the original. Usually, those who modify a game are owners of intellectual property or a third-party end user.

After that we provide introduction to the End-User License Agreements and Terms of Use that frequently are provided with video games and establish brief rules on copyright holders' desire or lack thereof for their intellectual property to be modified. Two different approaches to video game modification are explored, pertinent to companies' different attitudes toward modification by third parties and end users. The first is adopted by companies that encourage modification. This is demonstrated by terms in their EULA or Terms and Conditions. Some companies, such as Bethesda, also offer opportunities and incentives for third parties to modify their intellectual property. The second is taken by companies that want to discourage modifying, such as Nintendo, which illustrates this through aggressive litigation, strict EULAs, and Terms and Conditions covering their property.

Furthermore, issues and risks with respect to modifying are explored through potential breach of contract, copyright infringement, and reverse engineering. Breach of contract may arise when terms of the copyright holder's EULA or Terms of Use are violated. An example of breach of contract and its remedy is discussed in the case of *iRacing.com Motorsport Simulations, L.L.C. v. Robinson, Micro Star v. FormGen Inc.*, where a third-party user violated the copyright holder's EULA and the court awarded only nominal damages. Copyright infringement will be implicated where the end user has exceeded the scope of their license, and exercises an exclusive right reserved for the copyright owner, as was in the case *Micro Star v. FormGen Inc.*, where the court held that a third party infringed upon the copyright holder's intellectual property by selling and distributing a modification without permission. Reverse engineering is a process which may involve a copyrighted item being dismantled and used to create a new product. Reverse engineering can be useful, as well as harmful. *Blizzard Entertainment, Inc. v. Reeves* illustrates how reverse engineering may be used as a vehicle for copyright infringement.

The defense of fair use is analyzed in counterexamples to *iRacing.com Motorsport Simulations, L.L.C., Micro Star* and *Blizzard Entertainment, Inc.*, where the court essentially found in favor of the modifiers. These include the cases of *Sony Computer Entertainment Inc. v. Connectix Corp.*, and *Sega Enterprises Ltd. v. Accolade, Inc.*, where the modifiers successfully pleaded fair use in their reverse engineering of a copyright protected product, and *Nintendo of America, Inc. v. Lewis Galoob Toys, Inc.*, where the court found all the factors of fair use weighed in favor of the modifier.

Finally, gaps in the law are shown in the cases of *MDY Industries, L.L.C. v. Blizzard Entertainment Inc.,* where a prohibition on cheating predated the use of bots that gave players unfair advantages, and the case of DoTA, where open-source code led to the copyright holder, Blizzard, losing their intellectual property rights to their competitor, Valve.

When considering the legal ramifications of video game modding, numerous balancing interests between copyright holders and end users or third-party modifiers must be taken into account. On the one hand, it is the right of copyright holders to protect their intellectual property and determine how much of their work they are willing to license out, or whether they are willing to license it out at all. On the other, third-party end users may want to customize games to best benefit from the creation or want to reverse engineer them in order to make something entirely new. In addition to accommodating these two interests, as technology rapidly develops sometimes, it is difficult for the law to provide the most equitable remedy when technology faces new unanticipated challenges.

Legal Concept of Video Game Modding

What Are Video Game Modifications

There are different ways to define video game modification. The 9th Circuit in *Nintendo v. Galoob* refers to video game modification as being a derivative work that exists in permanent or concrete form.[1] Under 17 U.S.C. § 101, a derivative work is a "A copyrightable creation that is based on a preexisting product; a translation, musical arrangement, fictionalization, motion-picture version, abridgment, or any other recast or adapted form of an original work. Only the holder of the copyright of the original form can produce or permit someone else to produce a derivative work."[2] According to an article by Lindstrom (2020), video game modifications "[i]n the video game industry, is 'the act of changing a game, usually through computer programming, with software tools that are not part of the game.'" To elaborate on this definition, in an article by Wallace (2019), "Modding is the process of altering, adding to, or deleting video game code to change the way that a particular game is played."

What Law Governs Mods

The most pertinent statutes regarding video game modifications fall under the copyright statute, U.S.C. Title 17 Copyrights. Categories of protected works fall under 17 U.S.C. § 102 Subject matter of copyright. There is no video game specific statute, and thus different aspects of a video game are covered by different parts of the law. The program code of a video game is protectable as a literary work under 17 U.S.C. § 102 (1) literary works.[3] A video game's image data is protectable as a pictorial, graphic, and sculptural work under 17 U.S.C. § 102 (5).[4] The sounds of a video game are protectable under 17 U.S.C. § 102 (7) sound recordings, and the gameplay as experienced by a player is potentially protectable under 17 U.S.C. § 102 (6) Motion pictures and other audiovisual works.[5] Once a game has been developed and copyright protected, the video game modification, or derivative work, that ends

1 Lewis Galoob Toys, Inc. v. Nintendo of America, Inc., 780 F.Supp. 1283 (N.D.Cal.1991).

2 Garner, B. A. (2019). Derivative work. In *Black's Law Dictionary*. (11th ed.).

3 17 U.S.C.A. § 102 (West).

4 Id.

5 Id.

up getting litigated will likely implicate copyright infringement, because in video game modification suits, the modifier is usually a third-party user who is creating a derivative work of copyrighted subject matter without a license from the owner.

Examples of Modifications

Both the copyright holder and third parties can create modifications. There are many different uses and purposes of video game modifications. This can range from "minor bug fixes, to complete overhauls rendering the underlying game all but unrecognizable." (Lindstrom, 2020). On one end of the spectrum, a video game modification can be something minor, such as a developer manually rewriting a part of the game's source code to fix an issue. (Allamanis et al., 2021). An example of a minor modification is a bug fix, such as New World's 1.3.2 Patch Update. In the update, the copyright owners corrected a small issue within the game "where the same player could be listed multiple times on [a]... roster list."[6]

Other modifications can be simple aesthetic changes that players want to see in a game. Another example is the number of different types of modifications available for Electronic Arts' game, The Sims4. The Sims4 is a "simulation game that gives you the power to create and control people," like a virtual dollhouse.[7] Modifications available for The Sims4 range from offering different heights, growing an automatic beard, to different types of furniture not offered in the base game.[8] The popular game Minecraft also has a large modding community and offers numerous aesthetic changes. Some examples include offering items for interior decorating such as different types of tables and chairs not available in the base game (https://www.minecraftmods.com/). Other functional modifications available to download include the ability to tame wild animals and adding a hygiene bar for your player to make identifying their needs easier.

On the other end of the spectrum of video game modifications, an original work can be changed so much that the final product is nearly unrecognizable from its original form. An example of this is the game Defense of The Ancients (DoTA). A third-party end user created DoTA as a modification derived from the game Warcraft III's map editor and became so successful it eventually branched off into its own game.[9] Another example is the community that made the Enderal: Forgotten Stories modification.[10] Enderal is a modification of a Bethesda game, Skyrim, that was altered so extensively it became its own game with completely different characters, settings, and storylines.

While it is the right of copyright holders to modify video games any way they want, issues may emerge when third-party users create modifications. It is the right of the copyright owners to determine how much of their software they are willing to license out to end users or whether they are willing to license any of it out at all. The degree to which copyright holders are willing to allow end users to alter their property is usually outlined in an End User License Agreement or their Terms of Use.

---

6 Amazon.com Services L.L.C. (2022, February 8). *New World Update 1.3.2.* https://www.newworld.com/en-us/news/articles/new-world-update-1-3-2#ags-MediaPopup

7 Electronic Arts Inc. (n.d.). *The Sims 4.* Retrieved February 23, 2022, from https://www.ea.com/games/the-sims/the-sims-4

8 Horti. S., Morton, L., & Webber, J.E. (2022, August 31). *The best Sims 4 mods in 2022.* PC Gamer. https://www.pcgamer.com/best-sims-4-mods/

9 Dean, P. (2014, April 14). *The Story of Dota*. Eurogamer. https://www.eurogamer.net/articles/2011-08-16-the-story-of-dota-article

10 Steam. (n.d.). *Enderal: Forgotten Stories (Special Edition).* Valve Corporation. Retrieved February 23, 2022, from https://store.steampowered.com/app/976620/Enderal_Forgotten_Stories_Special_Edition/

End User License Agreement and Terms of Use

"An End-User License Agreement (EULA), also known as 'tear open,' or 'box top' or 'shrink-wrap' license agreement is the document that purports to form a contract between the mass market software developer and end-user." (Lutten & Wilf, 2021). In addition to EULAs, video game companies will typically provide Terms of Use via click wrap agreements. Click wrap agreements "require a user to consent to any terms or conditions by clicking on a dialogue box on a screen in order to proceed with an internet transaction." (Gans, Krause, & Speiser, 2022). EULAs and Terms of use will generally include a variation of a license grant, prohibition against disassembly, prohibition against resale or renting, choice of forum and law/binding arbitration, and, at the end, an agreement for the consumer who uses the software to agree to the terms outlined (Gans, Krause, & Speiser, 2022).

In EULAs and Terms of Use agreements, companies will outline provisions that address how much of their software they are licensing to the end user. These include provisions stipulating whether or not user generated content is permissible, whether sharing is acceptable, whether user generated content and sharing can be done for a fee, or cannot be done freely, and some companies offer to provide that editing tools and forums for creation and content sharing. Other companies may expressly forbid any type of user generated content and sharing.

Companies That Encourage Modding

Some video game companies encourage modifications by providing provisions in their Terms of Use and/or EULA as well as copyright owner generated tools to create third-party end-user generated content. Bethesda's EULA specifically addresses video game modifications in its terms of service:

> The term "Game Mod" means downloadable, user-generated Content developed or created by You or a third party using an Editor Tool (as defined below). In certain cases, as determined by ZeniMax, Game Mods may be made available to other users of a Service or a Game and in such cases, such other users may download the Game Mods from ZeniMax or third parties and use such Game Mods in connection with playing a Game or receiving a Service from ZeniMax.[11]

According to Bethesda's EULA, ZeniMax, the copyright owner, provides editing tools for end users to create their own user generated content, and allows for those third-party modifications to be "made available to other users," thus facilitating creation and sharing.[12]

Apart from its EULA, Bethesda also offers opportunities for video game modifiers to share and get paid for their creations for certain games, through its Creation Club. Creation Club's website states, "Creation Club is a collection of all-new content for both Fallout 4 and Skyrim. It features new items, abilities, Bethesda Games Studios created gameplay, and outside development partners including the best community creators. Creation Club content is fully curated and compatible with the main game and official add-ons."[13] Skyrim, in particular, has over 45,000 mods available on the Nexusmods sharing platform. According to an article from Geforce, Skyrim is one of the most mod-

[11] Zenimax Media Company. (2021, December 13). *Bethesda Terms of Service*. Bethesda Softworks L.L.C.. Retrieved February 23, 2022, from https://bethesda.net/en/document/terms-of-service

[12] Id.

[13] Bethesda. (n.d.). *Creation Club.* Bethesda Softworks L.L.C.. Retrieved February 23, 2022, from https://creationclub.bethesda.net/en

ded games, and this contributes to its continual market success despite it being released several years ago.[14] Bethesda encourages and facilitates modifications created by end users, by offering incentives, offering sharing platforms, and giving third-party end users the opportunity to work with the owners to create and share content.

Like Bethesda, Electronic Arts also addresses and encourages third-party end-user generated modifications by providing provisions addressing user generated content. This shows that Electronic Arts anticipates third-party end-user modification creation and sharing. Their user generated content provision states:

> When you contribute UGC, you grant to EA, its licensors and licensees... sublicensable license to use, host, store, reproduce, modify, create derivative works, publicly perform, publicly display or otherwise transmit and communicate the UGC... You also grant to all other users who can access and use your UGC on an EA Service the right to use, copy, modify, display, perform, create derivative works from, and otherwise communicate and distribute your UGC on or through the relevant EA Service...[15]

Electronic Arts further encourages third party end user created modifications by making it easy for users of certain games to share and download modifications. For example, Electronic Arts offers this for their game, The Sims 4. In Maxis Policy on Mods, Electronic Arts "strives to support the creativity of our community. We know that, for many of you, Mods are an important part of your game experience. For that reason, [Electronic Arts] support a framework in The Sims 4 that makes it easier for [players and end users] to install and use Mods."[16] Like Bethesda, Electronic Arts encourages third party end user generated content, and offers tools that make it easy to share content with other players.

Bethesda's and Electronic Arts' policies illustrate that there is an approach where some copyright owners encourage modification creation and sharing. In addition to Bethesda and Electronic Arts' approaches to modification, other companies encourage modifying by offering mod competitions. Modding competitions invite third-party end users to share their creativity for a monetary prize. An example of this was Nvidia's 'Make Something Unreal Competition 2004', which was conducted in association with Epic Games and Atari. For the competition, third-party developers were invited to submit modifications intended to be played in an 'Unreal Tournament' for a prize of $1,000,000.[17] The best modifications were made available for third parties and end users to download from Epic Games' website and were compatible with gameplay. In addition to the prize fund, the sponsors also offered the winner the opportunity to work with Epic Games developers or create a commercial version of the modification and publish it as a separate independent entity.[18]

Discouraging Modding

In contrast to companies that offer tools, encourage modifying communities, and create competitions, at the other end of the modification spectrum, there are some companies that expressly limit

[14] Dyer, A. (2016, March 18). *PC game mods — From smurfs to counter strike and beyond.* NVIDIA. https://www.nvidia.com/en-us/geforce/news/history-of-pc-game-mods/

[15] Electronic Arts. (n.d.). *Electronic Arts User Agreement*. Retrieved February 23, 2022, from https://tos.ea.com/legalapp/WEBTERMS/US/en/PC/#section10

[16] Electronic Arts. (n.d.). *The Sims 4 — Mods and game updates.* https://help.ea.com/en/help/the-sims/the-sims-4/mods-and-the-sims-4-game-updates/

[17] Epic Games. (n.d.). *Make something unreal*. Retrieved February 23, 2022, from https://docs.unrealengine.com/udk/Two/MakeSomethingUnreal.html#FAQ

[18] Epic Games. (n.d.).

third-party modification, creation, and sharing. According to an article by Wilson Sonsini Goodrich & Rosati, a legal technology firm, video game copyright owners take different approaches to encouraging or discouraging third-party modifications.[19] On the encouraging end of the spectrum, companies like Bethesda offer tools and opportunities for third parties to work with copyright owners, in addition to the possibility of being compensated for their creations. In contrast to Bethesda's, Electronic Arts', and Nvidia's policies on video game modification by end users and third parties, which encourage and facilitate the creation and sharing of modifications, there are companies that discourage third-party end-user generated content sharing. For example, Nintendo Switch's current EULA discourages modification and reverse engineering by explicitly stating, "(4) You may not copy, duplicate, publish, transmit publicly, lease, modify or reverse engineer the Software. (5) You may not illegally modify this Nintendo video game system itself, its peripheral equipment or the Software, or may not use any peripheral equipment of this Nintendo video game system or any software which are not authorized by Nintendo."[20] As illustrated, Nintendo Switch's EULA prohibits end users from modifying or reverse engineering their software. In contrast to Bethesda's, Nintendo's EULA also lacks a provision addressing user-generated content and sharing, further positing that Nintendo discourages third-party end-user modification and sharing.

In Wilson Sonsini Goodrich & Rosati's article on video game modification, is described as a company with a "No Modding Approach," which is "famous for taking aggressive action to defend its intellectual property rights" by sending cease and desist letters to modifiers.[21] Nintendo has even shut down largely popular gaming tournaments. In 2020, Nintendo sent the producer of the large Super Smash Brother's Online Tournament, BigHouse, a cease-and-desist letter, and BigHouse cancelled the tournament in response. Nintendo stated that the online tournament would require the use of an unauthorized modifications to play online and insisted that it had no choice but to protect its intellectual property rights.[22] The modification was likely required because Super Smash Brothers Melee is not playable online. However, this cancellation supports Wilson Sonsini Goodrich & Rosati's statement that Nintendo has a no modding approach toward game modification. This is evident because the tournament Nintendo essentially shut down brought Nintendo fans and users together to play its game in a hugely anticipated tournament.

Additionally, in a modification article by Murty (2020), intellectual property lawyers opine that Nintendo is aggressive in sending out cease-and-desist letters to such a degree that it may even face a backlash.[23] In 2020, Nintendo sent a cease-and-desist letter to a charity being held for a streamer who died by suicide.[24] As part of the charity event, custom JOY-CON controllers were being sold to raise suicide awareness. Nintendo owns the intellectual property rights to JOY-CON controllers, and the charity had modified the controllers by customizing their appearance. Nintendo sent a cease-and-desist letter to the charity organizers, who could no longer sell the merchandise as a result.[25]

[19] Krosnicki, J, McKinney, S, & Shevall, A. (2020, July 20). *Are gaming companies maddened by mods or embracing them?* JD Supra. https://www.jdsupra.com/legalnews/are-gaming-companies-maddened-by-mods-51053/#25

[20] Nintendo. (n.d.). *Nintendo Switch Support: End User License Agreement.* Retrieved February 23, 2022, from https://www.nintendo.com/sg/support/switch/eula/usage_policy.html

[21] Krosnicki, J. et al (2020).

[22] Good, O. S. (2020, November 19). *Smash Bros. Tournament the Big House 10 canceled over Netcode*. Polygon. https://www.polygon.com/2020/11/19/21578200/super-smash-bros-tournament-the-big-house-10-canceled-nintendo-c-d

[23] Murty, P. (2020, December 8). *Nintendo faces backlash over cease & desist letters*. Smith & Hopen. https://smithhopen.com/2020/12/09/nintendo-faces-backlash-over-cease-desist-letters/

[24] Murty, 2020.

[25] Id.

The author of the article concludes that, although Nintendo had the right to protect its intellectual property Nintendo incurred a "huge PR backlash" by shutting down a charity, which may serve as a cautionary tale about taking aggressive action against third-party end-user generated content.[26]

Issues and Risks with Modifying

Different companies' attitudes towards video game modification are reflected in the provisions included (or not included) in their EULAs and Terms of Use.[27]. Nintendo illustrates that unauthorized alterations to protected works can result in modifiers receiving cease-and-desist letters from the copyright holders. For companies that encourage modifying, such as Electronic Arts and Bethesda, issues will emerge if end users exceed the scope of their limited license in using the copyright owner's software or violate the covenants and conditions in their terms.

Breach of Contract

Breach of contract may arise when a condition or term of a copyright holder's EULA or Terms of Use is violated. The terms in an agreement can either be covenants or conditions. When a copyright holder grants a nonexclusive, limited license to end users to use their software, the contractual terms that "limit a license's scope are 'conditions.'"[28] "All other license terms are 'covenants' that are actionable under contract law."[29] Typically, the EULA or Terms of Use will state which jurisdiction's laws will apply in contractual disputes because contract law is governed by state law. The EULA and Terms of Use can also state whether disputes will be arbitrated. Some provisions will expressly state that end users must make their claims in small claims court and put limitations on recoverable damages.[30]

Damages for an end user's breach of contract for violating the copyright owner's EULA or Terms of Use are generally minimal in comparison to the remedies available for copyright infringement claims. Some notable differences are that in a copyright claim the prevailing party can seek attorney's fees, while in a breach of contract claim, each side normally bears the cost of attorney's fees on their own.[31] Additionally, contract damages can be minimal. Many video game's Terms of Use limit the amount of damages that are claimable.[32] The amount recoverable may be how much the game cost,

---

26 Murty, 2020.

27 The EULA and Terms of Use examples provided in this essay relative to Electronic Arts, Bethesda and Blizzard are U.S. based companies. While Electronic Arts and Bethesda tend to follow a mod freely approach, Blizzard in comparison has stricter guidelines. Additionally, in the example of Nintendo, a Japanese based company, it is hypothesized in Are Gaming Companies Maddened by Mods or Embracing Them?, by Wilson Sonsini & Rosati, that Nintendo's stricter approach to modification is influenced by Japan's approach to modding generally, as "[t]he Japanese government recently expanded regulations under its Unfair Competition Prevention Law to make modding game save data and game consoles punishable by up to five years in jail and up to $46,000 in fines."

28 MDY Indus., L.L.C. v. Blizzard Ent., Inc., 629 F.3d 928, 939 (9th Cir. 2010), as amended on denial of reh'g (Feb. 17, 2011), opinion amended and superseded on denial of reh'g, No. 09-15932, 2011 WL 538748 (9th Cir. Feb. 17, 2011).

29 Id.

30 Ellison, S. J. (2022, February 2). *Can I sue a video game creator or company?* https://www.findlaw.com/consumer/consumer-transactions/can-i-sue-a-video-game-creator-or-company-.html

31 Electronic Frontier Foundation. (2008, August 13). *Condition or covenant, and why should you care?* https://www.eff.org/deeplinks/2008/08/condition-or-covenant-and-why-should-you-care

32 Ellison, 2022.

or "for an online game the amount you paid the previous year."[33] An example of a limitation on recovery was illustrated in *iRacing.com Motorsport Simulations, L.L.C. v. Robinson*. In the Massachusetts District Court case, a third-party end user reverse engineered NASCAR 2003, a copyright protected game, in violation of the copyright holder's EULA, and the court only permitted nominal damages, or one dollar ($1.00) for the breach.[34]

Another example of breach of contract remedies for violating a video game's terms occurs when a copyright owner's software is used in excess. Some companies' terms can include a clause for the case of over deployment of property. This means that companies may anticipate their property being used on only one computer at a time. When over deployment occurs, or software is used on multiple computers, the remedy for this breach of covenant is repayment of the amount of additional licenses.[35]

Copyright Infringement

When an end user violates a condition of the copyright holder's EULA or Terms of Use, copyright infringement will be implicated if the end user has exceeded the scope of the license and has exercised an exclusive right reserved for the copyright owner.[36] Video game modifiers potentially infringe on the rights of copyright owners when they take a copyright protected original and make a derivative work from it. Under 17 U.S.C.§106, exclusive rights of copyright holders include reproducing the work in copies, creating derivative works, distributing copies, and, in the case of literary, musical and audiovisual works, displaying the work publicly.[37] Issues with respect to modifying emerge when third-party end users take an original work, and make a derivative from it. This includes modifying any part of the protected work, which encompasses virtually all modifications.

Micro Star v. FormGen Inc is an example of case where a copyright owner sued a third-party modifier because of user generated content.[38] In this case, a third-party modifier, Micro Star, compiled 300 user generated modifications, or additional player-created levels, of FormGen's Duke Nukem video game, copied them onto a CD, and then sold it commercially as Nuke It.[39] The modifier also took screen shots of images from the video game to decorate the packaging of the box that the compilation was sold in. In finding in favor of FormGen, the court took into account that Micro Star had replicated images from Duke Nukem gameplay on Nuke It's packaging without a license from FormGen and commercially profited from distributing the work.[40] Micro Star argued that it had not infringed on FormGen's copyright because FormGen gave end users a license to create and share their own created levels of the game. The court ultimately granted FormGen a preliminary injunction against Micro Star, requiring it to cease selling and distributing the modification. This ruling was based, in part, on Form Gen's license to end users, which allowed players to create and share their own levels, but also stipulated that "any new levels the players create must be offered to others solely for free."[41]

33 Ellison, 2022.

34 iRacing.com Motorsport Simulations, L.L.C. v. Robinson., (Mass. Dist. Ct. 2005) Case No. 1:05-cv-11639-NG.

35 Fulmer, P. (2019, September 30). *United States: Covenant or condition: When can a licensor sue its licensees for copyright infringement?* Mondaq. https://www.mondaq.com/unitedstates/licensing-syndication/849364/covenant-or-condition-when-can-a-licensor-sue-its-licensee-for-copyright-infringement

36 MDY Indus., L.L.C. v. Blizzard Ent., Inc., 629 F.3d 928, 939 (9th Cir. 2010).

37 17 U.S.C.§106 Exclusive rights in copyrighted works.

38 Micro Star v. FormGen Inc., 154 F.3d 1107 9th Cir.

39 Id.

40 Id. at 1113.

41 Id.

FormGen's approach to modding stands in contrast to Bethesda's system and Nintendo's. While Bethesda encourages and facilitates third-party generated modification, and Nintendo has an aggressive no third-party modification approach, FormGen suggests an intermediate category: selective enforcement. According to Wilson Sonsini Goodrich & Rosati's article, this intermediate approach to modifying occurs when copyright owners selectively "come after certain modders such as those mods designed to promote cheating or the insertion of inappropriate content."[42] Expanding on Wilson Sonsini Goodrich's & Rosati's description of the type of modifiers copyright owners will come after, this list should also include third-party modifiers that commercially profit while stealing potential customers from the copyright owners. In the case of *Microstar,* FormGen provided third-party end users with tools to be creative with their software and to create and share their own levels of Duke Nukem. However, when *Microstar* compiled user generated content and sold it commercially, the copyright owners chose to litigate. This illustrates an approach to third-party modifications, where the copyright owners may license and facilitation third-party modifications, but also demonstrates that, if modifiers' activities pass a point where copyright owners consider that they have overstepped the license, the copyright owner may choose to allege infringement.

Reverse Engineering

"Reverse engineering is the process [where] a copyrighted item is dismantled from the end product and reformulated to create another product..."[43] Reverse engineering can occur in several different ways. With respect to the gaming industry, this can involve unauthorized copying of copyright protected software onto a third party's computer in order to understand it and/or modify it to create a derivative work. When this occurs, copyright infringement may be implicated because copying is an exclusive right reserved for the owner.

Blizzard is another company that encourages and facilitates third-party user generated modifications but has litigated against end users that have overstepped the license to modify. Blizzard allows a degree of space for third-party end users to create modifications. For example, Blizzard offers a Warcraft III editor that allows third parties and end users to create their own maps for gameplay. [44] According to the current EULA for Blizzard's BattleNet gaming platform, while Blizzard provides third party modifiers and end users forums and editing tools to modify certain aspects of gameplay, it expressly prohibits unauthorized creation of derivative works, such as copying, reproducing, translating, reverse engineering, deriving source code from, modifying, disassembling, or decompiling.[45] The fact that Blizzard offers editing tools suggests that the company supports modification to a degree. However, their reservation of rights and provision against unauthorized derivative works also suggests that Blizzard anticipates the possibility of modifiers overstepping their license to use its software.

In the case of Blizzard Entertainment, Inc. v. Reeves, a third-party end user of World of Warcraft reverse engineered part of World of Warcraft's software to create a modification that allowed users to access World of Warcraft game servers and play without paying the required monthly subscription

[42] Krosnicki, J. et al (2020).

[43] Krosnicki, J, McKinney, S, & Shevall, A. (2020, July 20). *Are gaming companies maddened by mods or embracing them?* JD Supra. https://www.jdsupra.com/legalnews/are-gaming-companies

[44] Blizzard. (2020, August 27). *Revisiting the Warcraft III Editor.* Blizzard Entertainment Inc. https://news.blizzard.com/en-us/warcraft3/23395649/revisiting-the-warcraft-iii-editor

[45] Blizzard Entertainment Inc. (n.d.). *Blizzard end user license agreement.* Retrieved March 1, 2022, from https://www.blizzard.com/en-us/legal/fba4d00f-c7e4-4883-b8b9-1b4500a402ea/blizzard-end-user-license-agreement

fee, thus infringing on Blizzard's copyright.[46] In this case, the third-party modifier, Reeves, reverse engineered part of World of Warcraft code in order to create new servers that could access World of Warcraft servers without paying the subscription fee that is required to log in. Reeves offered other third parties access to her circumvention software on her website, scapegaming, in exchange for donations, which ended up totaling $3,052,339.[47] Blizzard requested damages under the 17 U.S.C § 1201 DMCA anti-circumvention statute, alleging that Reeves had infringed on their copyright when she offered the software through her website. Blizzard also claimed that, by copying and reverse engineering their property without authorization, Reeves had violated Blizzard's EULA and Terms of Use, and was thus in breach of contract.

The court ended up awarding Blizzard Reeve's $3,052,339 in profit as compensation for copyright infringement because Reeves had copied World of Warcraft's software to her own computer in order to modify so that World of Warcraft servers could be accessed while circumventing Blizzard's subscription fee. This constituted unauthorized copying, which is the exclusive right of copyright owners. Blizzard lost its claim for $20,886,200 ($2,500 per act of circumvention) for DMCA statutory violations because Blizzard could not prove that the 104,431 payments to Reeves for using the scapegaming website represented acts of circumvention, as the transactions did not reflect "the number of times that Plaintiff's anti-piracy mechanisms have been by-passed or the number of times that Defendant's servers performed their infringing services for users... [T]he quantity of transactions reflects the number of times people have paid money to Defendant — an act that is separate from a user's act of accessing Defendant's servers."[48]

The case of Blizzard Entertainment Inc. illustrates why some copyright holders may choose to expressly prohibit reverse engineering in their EULAs and Terms of Use. Reeves reverse engineering World of Warcraft's software resulted in her taking away Blizzard's revenue by circumventing its subscription fee. While this shows how reverse engineering can be a vehicle for copyright infringement, there are also instances where courts may allow for reverse engineering, as well as defenses against copyright infringement claims.

Defenses: Fair Use

Fair use is an affirmative defense against copyright infringement claims that involve unauthorized copying, modifying, or reverse engineering. In the case of Sony Computer Entertainment Inc. v. Connectix Corp., Connectix successfully pleaded fair use for its reverse engineering of Sony's PlayStation. Sony alleged Connectix had infringed on its copyright by reverse engineering its copyright protected game console. This involved altering the PlayStation's input-output system BIOS in order to make PlayStation games playable on personal computers.[49] In this case, Connectix engineers needed to copy Sony's input-output system BIOS onto a computer and disassemble object code into source code to produce a modification that allowed PlayStation games to be played on personal computers. Despite copying being an infringement of the copyright holder's exclusive rights, the court found that Connectix's copying was only an intermediary step. The court reasoned that reverse engineering was necessary to reach unprotected functional elements in the PlayStation, and that none of the copyrightable elements appeared in the final modification.[50]

[46] Blizzard Ent., Inc. v. Reeves, No. CV 09-7621 SVW AJWX, 2010 WL 4054095, at 4 (C.D. Cal. Aug. 10, 2010).

[47] Blizzard Ent., Inc. v. Reeves, No. CV097621SVWAJWX, 2010 WL 11508371, at 5 (C.D. Cal. July 22, 2010).

[48] Id.

[49] Sony Computer Ent., Inc. v. Connectix Corp., 203 F.3d 596, 601 (9th Cir. 2000).

[50] Id.

The Statute

The Fair Use statute is 17 U.S.C.A. § 107.[51] There are four factors that courts will use in analyzing a claim. The first is (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes. With regard to this factor, the court may inquire as to whether the use of the derivative work is commercial in nature, and whether its use is transformative in comparison to the original.[52] Typically, if the use is found to be noncommercial and the new work found to be transformative, this will favor a finding of fair use. The second factor is (2) the nature of the copyrighted work. With regard to this factor, courts may consider whether a work is creative or factual, and whether the work is published or unpublished. The more creative a work is, the more this favors fair use, and if the disputed work has already been published, this favors fair use because the copyright owner has had the opportunity to profit commercially. The third factor (3) involves the amount and substantiality of the portion used in relation to the copyrighted work as a whole and depends on the case. A small portion of a copyrighted work can be unfair, while using a substantial portion of a copyrighted work can favor fair use. The final factor (4) is the effect of the use upon the potential market for or value of the copyrighted work. When considering this factor, the harm done to the copyright protected work's market will be analyzed.[53] If the harm is great and results in lost profits, diverted sales, or lost licensing revenue for the copyright owner, this will disfavor a finding of fair use.[54] Of the four factors, no single factor is dispositive to finding fair use, and the Supreme Court has cautioned that it should be applied on a case-by-case basis.[55]

In a case similar to that of Sony Computer Entertainment, Inc., Sega Enterprises Ltd. v. Accolade, Inc. involved reverse engineering. In this proceeding, the court analyzed Accolade's derivative work using fair use analysis and "concluded that where disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law."[56] In this case, Accolade reverse engineered Sega's gaming console, Genesis, in order to create video games that were compatible with Sega's console. Just like Sony Computer Entertainment, Inc., Sega alleged copyright infringement for the unauthorized copying of Genesis' code, as Accolade had saved Sony's files on multiple computers in order to disassemble it. The court found that Accolade had met the requirements for fair use, despite the "intermediate copying done... [falling] squarely within the category of" acts prohibited by the copyright statute.

With respect to the first factor, which involves character and purpose, the court found that Accolade's direct purpose "was... to study the functional requirements for Genesis compatibility so that it could modify existing games and make them usable with the Genesis console. Moreover...no other method of studying those requirements was available to Accolade...[additionally,] Accolade copied Sega's code for a legitimate, essentially non-exploitative purpose, and that the commercial aspect of its use can best be described as of minimal significance.[57] Thus the first factor favored fair use. With respect to the second factor, the nature of the copyrighted work, the court reasoned that

[51] 17 U.S.C.A. § 107, 17 USCA § 107.

[52] Cunard, J.P., Keller, B.P., & Potenza, M. (2022). *Copyright Fair Use, Practical Law Practice Note 2-523-3404.* Thomson Reuters. https://uk.practicallaw.thomsonreuters.com/2-523-3404?transitionType=Default&contextData=(sc.Default)

[53] Cunard et al. (2022).

[54] Cunard et al. (2022).

[55] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 577 (1994).

[56] Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510, 1527–28 (9th Cir. 1992), as amended (Jan. 6, 1993).

[57] Id. at 1522.

because disassembly was required and some of Sega's programs contained unprotected "aspects that cannot be examined without copying," it would be subject to less protection than traditional literary works, and found this factor favored fair use. With respect to the third factor, the amount and substantiality copied, the court reasoned that, by disassembling the console, Accolade had used the entire work, and thus this factor disfavored a finding of fair use. With respect to the fourth factor, which considers the effect of the use upon the market in relation to the copyrighted work, the court distinguished this case from *Harper and Row*, where the usurpation of a copyright holder's market was dispositive.[58] Here, though Accolade entered Sega's gaming market by selling games compatible with Sega, the court reasoned that introducing a new game would not necessarily usurp Sega's games, as purchasers could buy both, and found in favor of Accolade.[59]

The cases of Sony Computer Entertainment, Inc. and Sega Enterprises Ltd. v. Accolade, Inc. illustrate instances where modifiers have successfully raised fair use when the defendants were involved with reverse engineering of the plaintiff's copyright protected systems. In both cases, the disassembly of the copyright owner's consoles was necessary: in the first case, in order to make Sony games playable on other platforms, and in the latter case, in order to develop video games compatible with Genesis, which benefitted purchasers. These cases stand in contrast to the case of Blizzard Entertainment, where the modifier reverse engineered Blizzard's video game in order to circumvent subscription fees, and in addition, improperly cut into Blizzard's revenue by offering the derivative work. These cases show that there is a thin line between what the court will find permissible versus what is illegal.

Nintendo of America, Inc. v. Lewis Galoob Toys, Inc. is another case where a court found fair use in a copyright infringement case. In the case, Lewis Galoob Toys created the Game Genie, "an electronic device allowing NES (Nintendo Entertainment System) owners to change aspects of NES video games.[60] For example, the Game Genie would permit a video game character to run faster, jump higher, or become immortal."[61] According to Game Genie's website, there is a list of various cheats available for different games.[62] For Mario Brothers, the cheats include infinite lives, running faster, "Mega-jumping" and "Mega fast baddies."[63] In analyzing the Game Genie with respect to the four factors of fair use, under the first factor, character and purpose, the 9th Circuit Court found that this factor favored a finding of fair use because Nintendo had already published the games prior to the release of the Game Genie, thus it could benefit from it being on the market.[64] For the second and third factors, the court also favored a finding of fair use. The court compared end users' use of Game Genie to how Betamax users in *Sony Corp. of America v. Universal City Studios, Inc.* copied TV programs in their entirety.[65] The court reasoned that "consumers are not invited to witness Nintendo's audiovisual displays free of charge" and, despite Game Genie totally encompassing Nintendo's copyright, displays did not "militate against a finding of fair use."[66] For the fourth factor, which was considered

58 Harper & Row 471 U.S. at 562, 105 S.Ct. at 2231.

59 Sega, 977 F.2d.

60 Nintendo of Am., Inc. v. Lewis Galoob Toys, Inc., 16 F.3d 1032, 1033 (9th Cir. 1994).

61 Id.

62 GameGenie.com. (n.d.). *Nintendo (game genie) codes — Mario Bros*. Danworld, Inc. Retrieved March 3, 2022, from https://www.gamegenie.com/cheats/gamegenie/nes/mario_bros.html

63 Id.

64 Nintendo of Am., Inc. v. Lewis Galoob Toys, Inc., at 970.

65 Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 104 S. Ct. 774, 78 L. Ed. 2d 574 (1984).

66 Nintendo of Am., Inc. v. Lewis Galoob Toys, Inc., at 971.

the most significant, the court found that Nintendo failed to show market harm.[67] The court noted that Nintendo had not issued altered versions of games like Game Genie, nor had they established that they were going to enter that market, so it favored fair use for Lewis Galoob Toys, Inc.[68]

The rulings in the Sony Computer Entertainment Inc., Sega Enterprises Ltd., and Nintendo of America, Inc. reverse engineering modification cases differ from that in the Blizzard Entertainment case. These four cases represent a gray area for copyright holders and licensees/third party end users, where the court balances the rights of copyright holders with the rights of licensees and third-party end user to promote "the progress of science and the useful arts."[69] In the first cases, the courts found that the modifier's exercise of the copyright holder's exclusive rights was fair, while in the last, they found the derivative work to be inequitable. While all these cases had third-party modifiers committing an infringing activity in common, the different outcomes illustrate how developing technology does not always fall neatly within the law.

Gaps in the Law

A gap in the law can occur when an issue arises that lacks precedent or statutes to follow. As gaming technology advances, sometimes it is difficult for issues to fall neatly within the law. Two issues are: unanticipated advances in technology that go against the copyright owner's terms, and ownership over modifications. The following examples both pertain to Blizzard's game, World of Warcraft. Under the first issue, a third-party end user made a bot that altered World of Warcraft gameplay in violation of the copyright owner's EULA. However, Blizzard did not initiate anti-bot measures until the year after the modifier's bot was used. Under the second issue, a third party created the Defense of the Ancients game using licenses from Blizzard. Valve later employed the owner of the modification, and the owner eventually sold the rights to Valve, causing Blizzard to lose some of its property rights.[70]

MDY Industries, LLC v. Blizzard Entertainment Inc.

In *MDY Industries, LLC v. Blizzard Entertainment, Inc,* a third-party end user of World of Warcraft created a game modification software bot, Glider, that simulated game play while the user of the bot was not actually playing the game.[71] The purpose of using Glider was to gain experience, in game currency, and items, without the user of Glider actually having to actively play the game. The modifier initially only used Glider personally, but eventually created a website and sold the software online for $15 to $25 per license.[72] Blizzard alleged that, in addition to copyright infringement and contributory infringement of World of Warcraft, MDY's bot disrupted gameplay for other players because users of the bot were unfairly advantaged.[73] The court found that MDY was not contributorily liable for secondary infringement because Glider did not alter World of Warcraft's software in violation of copyright holder's rights. However, the modification did fall foul of 17 USC § 1201 Circumvention of

67 Nintendo of Am., Inc. v. Lewis Galoob Toys, Inc., at 971.

68 Id.

69 U.S. Const. art. I, § 8, cl. 8.

70 Orland, K. (2017, May 18). *Does Valve really own Dota? A jury will decide.* Ars Technica. https://arstechnica.com/gaming/2017/05/does-valve-really-own-dota-a-jury-will-decide/

71 MDY Indus., LLC v. Blizzard Ent., Inc., 629 F.3d 928, 936 (9th Cir. 2010).

72 Id.

73 Id.

copyright protection systems because Glider was designed to be undetected by World of Warcraft's anti-bot scanner.

MDY is a complex case that illustrates potential gaps in the law. The copyright owner wanted to protect World of Warcraft against third-party end user modifications that disrupted gameplay. Despite MDY's modification, MDY did not technically infringe Blizzard's exclusive rights, and Blizzard was unsuccessful in its copyright infringement claim. At the time of the dispute, World of Warcraft's terms of use expressly stated: "You agree that you will not ... (ii) create or use cheats, bots, 'mods,' and/or hacks, or any other third-party software designed to modify the World of Warcraft experience..."[74] MDY violated Blizzard's terms when it created the bot Glider. The court held that this violation was a breach of covenant under contract law, a promise to do or abstain from doing something, but did not actually violate the copyright holder's exclusive rights to prepare derivative works or exceed the scope of the license granted to end users. The court reasoned that to find a breach of Blizzard's terms of use as actionable under copyright infringement would essentially be allowing any software copyright holder to designate unfavorable conduct as infringement and would "allow software copyright owners far greater rights than Congress has generally conferred on copyright owners."[75] Though, in making this distinction, the court showed the balancing of rights between copyright holders and licensees, the outcome feels incomplete. MDY made over $6,000,000 selling Glider bots, despite the copyright holder's desire to ban the use of modifications to cheat.

MDY illustrates how advancing technology makes it difficult to enforce copyright owner's rights. MDY made the modification in 2004, but Blizzard did not release its anti-bot scanner until one year later, in 2005.[76] The release of anti-bot software at a later date could suggest that the technology was not anticipated when World of Warcraft was released because the Terms of Use drafted at that time showed that Blizzard desired to ban the use of modifications to cheat in the game. This shows that, while the desire to prohibit this conduct was anticipated at the release of World of Warcraft, technology was still advancing and not every type of modification could be adequately protected against. The copyright statute, which contains the cause of action Blizzard wanted against MDY, copyright infringement, was passed as a series of acts in 1976.[77] While Blizzard was unsuccessful in its copyright infringement claim, it was able to get an injunctive relief from the court under the Digital Millennial Copyright Act, or 17 USC § 1201. Potential gaps in the law are that the statue that Blizzard was able to receive relief under, violations regarding circumvention of technological measures, was not in effect until November 1999.[78] Had World of Warcraft been released just 5 years prior, Blizzard may not have had a remedy against MDY.

DoTA

DoTA delineates issues regarding modification ownership. As previously mentioned, the popular video game DoTA is a modification of Blizzard's Warcraft III. Blizzard's editing tools for modification, Warcraft's map editor tool, made DoTA's inception possible. From its creation in 2002, Blizzard licensed out intellectual property that was the starting point of several websites and variations of DoTA, such as DoTA Allstars.[79] Blizzard's competitor, Valve, then acquired DoTA Allstars's lead devel-

[74] Id.

[75] Id.

[76] Id.

[77] 17 U.S.C.A. § 103, 17 USCA § 103 (West).

[78] 17 U.S.C.A. § 1201, 17 USCA § 1201 (West).

[79] Notice of Opposition (Valve., Corp. v. Blizzard Ent., Inc.) ESTTA441431 (TTAB 2011), https://ttabvue.uspto.gov/ttabvue/ttabvue-91202572-OPP-1.pdf

oper in 2009. Later, Valve applied to the USPTO to trademark DoTA, which Blizzard opposed in 2011. Blizzard argued that DoTA had been created by years of reputation building, contact networking, intellectual property, and branding on the part of Blizzard, and allowing Valve to claim the trademark would unfairly appropriate all the work Blizzard associated with DoTA.[80] Blizzard lost its case, and Valve acquired the rights to DoTA. According to both Blizzard's and Valve's websites, the use of the DoTA trademark belongs to Valve, and Blizzard features DoTA on their website through a license obtained from Valve.

In addition to Blizzard and Valve's competition over the trademark, in 2017, Blizzard Entertainment and Valve Corporation were plaintiffs in a motion for summary judgment in a subsequent copyright infringement case, Blizzard Entertainment, Inc. v. Lilith Games (Shanghai) Co. Ltd. In that case, a third-party modifier and one of the original contributors to DoTA, Lilith Games, infringed DoTA's copyrights to create a mobile game, DoTA Legends and Heroes Charge.[81] The defendant in that case was one of the original modifiers of DoTA and argued that its mobile games were separate works and not derivatives of the copyright protected DoTA, which was owned by Valve. Lilith Games argued that Valve had no rights to subsequent works derived from DoTA, i.e., Lilith's mobile version, and moved for summary judgment. The court held that Valve had validly acquired the rights to DoTA from the original modifiers and "may recover for original expression that [the original modifiers] contributed to their versions of DotA and DotA Allstars, as well as original expression that Valve itself contributed to DotA 2."[82]

DoTA illustrates how complicated creating a successful modification and establishing rights can be. From its inception, Blizzard arguably encouraged and facilitated modifications when it licensed out DoTA to third parties. However, despite coming to a mutual agreement, where Blizzard retained the noncommercial rights to DoTA and Valve retained the commercial rights to the same game, it is unlikely that this was the outcome Blizzard wanted, given its opposition to Valve's application to trademark DoTA. In its opposition to the USPTO, Blizzard argued that allowing Valve to trademark DoTA would essentially be allowing Valve to appropriate Blizzard's goodwill, because DoTA was created from Warcraft III and had gained popularity and association with it for several years.[83] Blizzard further argued that allowing Valve to own the trademark would create a source of confusion for the same reason.[84]

Blizzard's provision of modification tools most likely created the environment that caused Blizzard to lose DoTA to Valve. One of the original developers of DoTA used the Warcraft III editing tool to create DoTA and made his creation available as open-source code. Subsequent modifiers built upon the modification, and Valve later acquired these creators. Ownership of the modification was further exacerbated in Blizzard Entertainment, Inc. v. Lilith Games (Shanghai) Co. Ltd., when one of the original creators, who had already sold his rights, tried to make a mobile DoTA game and reclaim the intellectual property that belonged to Valve. Blizzard has since updated its custom game acceptable use policy, which now reflects a conservative approach to modification. Blizzard's terms state that "ownership [of] custom games are and shall remain the sole and exclusive property of Blizzard."[85]

---

80 Orland (2017).

81 Blizzard Ent., Inc. v. Lilith Games (Shanghai) Co., No. 3:15-CV-04084-CRB, 2017 WL 2118342, at 8 (N.D. Cal. May 16, 2017).

82 Id. at 11.

83 Notice of Opposition (Valve., Corp. v. Blizzard Ent., Inc.) ESTTA441431 (TTAB 2011), https://ttabvue.uspto.gov/ttabvue/ttabvue-91202572-OPP-1.pdf

84 Id.

85 Blizzard Entertainment Inc. (n.d.). *Custom game acceptable use policy*. Retrieved March 1, 2022, from https://www.blizzard.com/en-us/legal/2749df07-2b53-4990-b75e-a7cb3610318b/custom-game-acceptable-use-policy

This could possibly be a reflection of its success and loss of DoTA, or purely a preventative measure, edging further away from strong encouragement of third-party end-user modifications.

The court ended up awarding Blizzard Reeve's $3,052,339 in profit as compensation for copyright infringement because Reeves had copied World of Warcraft's software to her own computer in order to modify so that World of Warcraft servers could be accessed while circumventing Blizzard's subscription fee. This constituted unauthorized copying, which is the exclusive right of copyright owners. Blizzard lost its claim for $20,886,200 ($2,500 per act of circumvention) for DMCA statutory violations because Blizzard could not prove that the 104,431 payments to Reeves for using the scape-gaming website represented acts of circumvention, as the transactions did not reflect "the number of times that Plaintiff's anti-piracy mechanisms have been by-passed or the number of times that Defendant's servers performed their infringing services for users... [T]he quantity of transactions reflects the number of times people have paid money to Defendant — an act that is separate from a user's act of accessing Defendant's servers."[86]

The case of Blizzard Entertainment Inc. illustrates why some copyright holders may choose to expressly prohibit reverse engineering in their EULAs and Terms of Use. Reeves reverse engineering World of Warcraft's software resulted in her taking away Blizzard's revenue by circumventing its subscription fee. While this shows how reverse engineering can be a vehicle for copyright infringement, there are also instances where courts may allow for reverse engineering, as well as defenses against copyright infringement claims.

Defenses: Fair Use

Fair use is an affirmative defense against copyright infringement claims that involve unauthorized copying, modifying, or reverse engineering. In the case of Sony Computer Entertainment Inc. v. Connectix Corp., Connectix successfully pleaded fair use for its reverse engineering of Sony's PlayStation. Sony alleged Connectix had infringed on its copyright by reverse engineering its copyright protected game console. This involved altering the PlayStation's input-output system BIOS in order to make PlayStation games playable on personal computers.[87] In this case, Connectix engineers needed to copy Sony's input-output system BIOS onto a computer and disassemble object code into source code to produce a modification that allowed PlayStation games to be played on personal computers. Despite copying being an infringement of the copyright holder's exclusive rights, the court found that Connectix's copying was only an intermediary step. The court reasoned that reverse engineering was necessary to reach unprotected functional elements in the PlayStation, and that none of the copyrightable elements appeared in the final modification.[88]

The Statute

The Fair Use statute is 17 U.S.C.A. § 107.[89] There are four factors that courts will use in analyzing a claim. The first is (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes. With regard to this factor, the court may inquire as to whether the use of the derivative work is commercial in nature, and whether its use is

86 Id.

87 Sony Computer Ent., Inc. v. Connectix Corp., 203 F.3d 596, 601 (9th Cir. 2000).

88 Id.

89 17 U.S.C.A. § 107, 17 USCA § 107.

transformative in comparison to the original.[90] Typically, if the use is found to be noncommercial and the new work found to be transformative, this will favor a finding of fair use. The second factor is (2) the nature of the copyrighted work. With regard to this factor, courts may consider whether a work is creative or factual, and whether the work is published or unpublished. The more creative a work is, the more this favors fair use, and if the disputed work has already been published, this favors fair use because the copyright owner has had the opportunity to profit commercially. The third factor (3) involves the amount and substantiality of the portion used in relation to the copyrighted work as a whole and depends on the case. A small portion of a copyrighted work can be unfair, while using a substantial portion of a copyrighted work can favor fair use. The final factor (4) is the effect of the use upon the potential market for or value of the copyrighted work. When considering this factor, the harm done to the copyright protected work's market will be analyzed.[91] If the harm is great and results in lost profits, diverted sales, or lost licensing revenue for the copyright owner, this will disfavor a finding of fair use.[92] Of the four factors, no single factor is dispositive to finding fair use, and the Supreme Court has cautioned that it should be applied on a case-by-case basis.[93]

In a case similar to that of Sony Computer Entertainment, Inc., Sega Enterprises Ltd. v. Accolade, Inc. involved reverse engineering. In this proceeding, the court analyzed Accolade's derivative work using fair use analysis and "concluded that where disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law."[94] In this case, Accolade reverse engineered Sega's gaming console, Genesis, in order to create video games that were compatible with Sega's console. Just like Sony Computer Entertainment, Inc., Sega alleged copyright infringement for the unauthorized copying of Genesis' code, as Accolade had saved Sony's files on multiple computers in order to disassemble it. The court found that Accolade had met the requirements for fair use, despite the "intermediate copying done... [falling] squarely within the category of" acts prohibited by the copyright statute.

With respect to the first factor, which involves character and purpose, the court found that Accolade's direct purpose "was...to study the functional requirements for Genesis compatibility so that it could modify existing games and make them usable with the Genesis console. Moreover...no other method of studying those requirements was available to Accolade...[additionally,] Accolade copied Sega's code for a legitimate, essentially non-exploitative purpose, and that the commercial aspect of its use can best be described as of minimal significance.[95] Thus the first factor favored fair use. With respect to the second factor, the nature of the copyrighted work, the court reasoned that because disassembly was required and some of Sega's programs contained unprotected "aspects that cannot be examined without copying," it would be subject to less protection than traditional literary works, and found this factor favored fair use. With respect to the third factor, the amount and substantiality copied, the court reasoned that, by disassembling the console, Accolade had used the entire work, and thus this factor disfavored a finding of fair use. With respect to the fourth factor, which considers the effect of the use upon the market in relation to the copyrighted work, the court

90 Cunard, J.P., Keller, B.P., & Potenza, M. (2022). *Copyright Fair Use, Practical Law Practice Note 2-523-3404.* Thomson Reuters. https://uk.practicallaw.thomsonreuters.com/2-523-3404?transitionType=Default&contextData=(sc.Default)

91 Cunard et al. (2022).

92 Cunard et al. (2022).

93 Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 577 (1994).

94 Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510, 1527–28 (9th Cir. 1992), as amended (Jan. 6, 1993).

95 Id. at 1522.

distinguished this case from *Harper and Row*, where the usurpation of a copyright holder's market was dispositive.[96] Here, though Accolade entered Sega's gaming market by selling games compatible with Sega, the court reasoned that introducing a new game would not necessarily usurp Sega's games, as purchasers could buy both, and found in favor of Accolade.[97]

The cases of Sony Computer Entertainment, Inc. and Sega Enterprises Ltd. v. Accolade, Inc. illustrate instances where modifiers have successfully raised fair use when the defendants were involved with reverse engineering of the plaintiff's copyright protected systems. In both cases, the disassembly of the copyright owner's consoles was necessary: in the first case, in order to make Sony games playable on other platforms, and in the latter case, in order to develop video games compatible with Genesis, which benefitted purchasers. These cases stand in contrast to the case of Blizzard Entertainment, where the modifier reverse engineered Blizzard's video game in order to circumvent subscription fees, and in addition, improperly cut into Blizzard's revenue by offering the derivative work. These cases show that there is a thin line between what the court will find permissible versus what is illegal.

Nintendo of America, Inc. v. Lewis Galoob Toys, Inc. is another case where a court found fair use in a copyright infringement case. In the case, Lewis Galoob Toys created the Game Genie, "an electronic device allowing NES (Nintendo Entertainment System) owners to change aspects of NES video games.[98] For example, the Game Genie would permit a video game character to run faster, jump higher, or become immortal."[99] According to Game Genie's website, there is a list of various cheats available for different games.[100] For Mario Brothers, the cheats include infinite lives, running faster, "Mega-jumping" and "Mega fast baddies."[101] In analyzing the Game Genie with respect to the four factors of fair use, under the first factor, character and purpose, the 9th Circuit Court found that this factor favored a finding of fair use because Nintendo had already published the games prior to the release of the Game Genie, thus it could benefit from it being on the market.[102] For the second and third factors, the court also favored a finding of fair use. The court compared end users' use of Game Genie to how Betamax users in *Sony Corp. of America v. Universal City Studios, Inc.* copied TV programs in their entirety.[103] The court reasoned that "consumers are not invited to witness Nintendo's audiovisual displays free of charge" and, despite Game Genie totally encompassing Nintendo's copyright, displays did not "militate against a finding of fair use."[104] For the fourth factor, which was considered the most significant, the court found that Nintendo failed to show market harm.[105] The court noted that Nintendo had not issued altered versions of games like Game Genie, nor had they established that they were going to enter that market, so it favored fair use for Lewis Galoob Toys, Inc.[106]

The rulings in the Sony Computer Entertainment Inc., Sega Enterprises Ltd., and Nintendo of America, Inc. reverse engineering modification cases differ from that in the Blizzard Entertainment

96 Harper & Row 471 U.S. at 562, 105 S.Ct. at 2231.

97 Sega, 977 F.2d.

98 Nintendo of Am., Inc. v. Lewis Galoob Toys, Inc., 16 F.3d 1032, 1033 (9th Cir. 1994).

99 Id.

100 GameGenie.com. (n.d.). *Nintendo (game genie) codes — Mario Bros.* Danworld, Inc. Retrieved March 3, 2022, from https://www.gamegenie.com/cheats/gamegenie/nes/mario_bros.html

101 Id.

102 Nintendo of Am., Inc. v. Lewis Galoob Toys, Inc., at 970.

103 Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 104 S. Ct. 774, 78 L. Ed. 2d 574 (1984).

104 Nintendo of Am., Inc. v. Lewis Galoob Toys, Inc., at 971.

105 Id.

106 Id.

case. These four cases represent a gray area for copyright holders and licensees/third party end users, where the court balances the rights of copyright holders with the rights of licensees and third-party end user to promote "the progress of science and the useful arts."[107] In the first cases, the courts found that the modifier's exercise of the copyright holder's exclusive rights was fair, while in the last, they found the derivative work to be inequitable. While all these cases had third-party modifiers committing an infringing activity in common, the different outcomes illustrate how developing technology does not always fall neatly within the law.

Gaps in the Law

A gap in the law can occur when an issue arises that lacks precedent or statutes to follow. As gaming technology advances, sometimes it is difficult for issues to fall neatly within the law. Two issues are: unanticipated advances in technology that go against the copyright owner's terms, and ownership over modifications. The following examples both pertain to Blizzard's game, World of Warcraft. Under the first issue, a third-party end user made a bot that altered World of Warcraft gameplay in violation of the copyright owner's EULA. However, Blizzard did not initiate anti-bot measures until the year after the modifier's bot was used. Under the second issue, a third party created the Defense of the Ancients game using licenses from Blizzard. Valve later employed the owner of the modification, and the owner eventually sold the rights to Valve, causing Blizzard to lose some of its property rights.[108]

MDY Industries, LLC v. Blizzard Entertainment Inc.

In *MDY Industries, LLC v. Blizzard Entertainment, Inc,* a third-party end user of World of Warcraft created a game modification software bot, Glider, that simulated game play while the user of the bot was not actually playing the game.[109] The purpose of using Glider was to gain experience, in game currency, and items, without the user of Glider actually having to actively play the game. The modifier initially only used Glider personally, but eventually created a website and sold the software online for $15 to $25 per license.[110] Blizzard alleged that, in addition to copyright infringement and contributory infringement of World of Warcraft, MDY's bot disrupted gameplay for other players because users of the bot were unfairly advantaged.[111] The court found that MDY was not contributorily liable for secondary infringement because Glider did not alter World of Warcraft's software in violation of copyright holder's rights. However, the modification did fall foul of 17 USC § 1201 Circumvention of copyright protection systems because Glider was designed to be undetected by World of Warcraft's anti-bot scanner.

MDY is a complex case that illustrates potential gaps in the law. The copyright owner wanted to protect World of Warcraft against third-party end user modifications that disrupted gameplay. Despite MDY's modification, MDY did not technically infringe Blizzard's exclusive rights, and Blizzard was unsuccessful in its copyright infringement claim. At the time of the dispute, World of Warcraft's terms of use expressly stated: "You agree that you will not ... (ii) create or use cheats,

[107] U.S. Const. art. I, § 8, cl. 8.

[108] Orland, K. (2017, May 18). *Does Valve really own Dota? A jury will decide.* Ars Technica. https://arstechnica.com/gaming/2017/05/does-valve-really-own-dota-a-jury-will-decide/

[109] MDY Indus., LLC v. Blizzard Ent., Inc., 629 F.3d 928, 936 (9th Cir. 2010).

[110] Id.

[111] Id.

bots, 'mods,' and/or hacks, or any other third-party software designed to modify the World of Warcraft experience..."[112] MDY violated Blizzard's terms when it created the bot Glider. The court held that this violation was a breach of covenant under contract law, a promise to do or abstain from doing something, but did not actually violate the copyright holder's exclusive rights to prepare derivative works or exceed the scope of the license granted to end users. The court reasoned that to find a breach of Blizzard's terms of use as actionable under copyright infringement would essentially be allowing any software copyright holder to designate unfavorable conduct as infringement and would "allow software copyright owners far greater rights than Congress has generally conferred on copyright owners."[113] Though, in making this distinction, the court showed the balancing of rights between copyright holders and licensees, the outcome feels incomplete. MDY made over $6,000,000 selling Glider bots, despite the copyright holder's desire to ban the use of modifications to cheat.

MDY illustrates how advancing technology makes it difficult to enforce copyright owner's rights. MDY made the modification in 2004, but Blizzard did not release its anti-bot scanner until one year later, in 2005.[114] The release of anti-bot software at a later date could suggest that the technology was not anticipated when World of Warcraft was released because the Terms of Use drafted at that time showed that Blizzard desired to ban the use of modifications to cheat in the game. This shows that, while the desire to prohibit this conduct was anticipated at the release of World of Warcraft, technology was still advancing and not every type of modification could be adequately protected against. The copyright statute, which contains the cause of action Blizzard wanted against MDY, copyright infringement, was passed as a series of acts in 1976.[115] While Blizzard was unsuccessful in its copyright infringement claim, it was able to get an injunctive relief from the court under the Digital Millennial Copyright Act, or 17 USC § 1201. Potential gaps in the law are that the statue that Blizzard was able to receive relief under, violations regarding circumvention of technological measures, was not in effect until November 1999.[116] Had World of Warcraft been released just 5 years prior, Blizzard may not have had a remedy against MDY.

DoTA

DoTA delineates issues regarding modification ownership. As previously mentioned, the popular video game DoTA is a modification of Blizzard's Warcraft III. Blizzard's editing tools for modification, Warcraft's map editor tool, made DoTA's inception possible. From its creation in 2002, Blizzard licensed out intellectual property that was the starting point of several websites and variations of DoTA, such as DoTA Allstars.[117] Blizzard's competitor, Valve, then acquired DoTA Allstars's lead developer in 2009. Later, Valve applied to the USPTO to trademark DoTA, which Blizzard opposed in 2011. Blizzard argued that DoTA had been created by years of reputation building, contact networking, intellectual property, and branding on the part of Blizzard, and allowing Valve to claim the trademark would unfairly appropriate all the work Blizzard associated with DoTA.[118] Blizzard lost its case, and

112 Id.

113 Id.

114 Id.

115 17 U.S.C.A. § 103, 17 USCA § 103 (West).

116 17 U.S.C.A. § 1201, 17 USCA § 1201 (Weast).

117 Notice of Opposition (Valve., Corp. v. Blizzard Ent., Inc.) ESTTA441431 (TTAB 2011), https://ttabvue.uspto.gov/ttabvue/ttabvue-91202572-OPP-1.pdf

118 Orland (2017).

Valve acquired the rights to DoTA. According to both Blizzard's and Valve's websites, the use of the DoTA trademark belongs to Valve, and Blizzard features DoTA on their website through a license obtained from Valve.

In addition to Blizzard and Valve's competition over the trademark, in 2017, Blizzard Entertainment and Valve Corporation were plaintiffs in a motion for summary judgment in a subsequent copyright infringement case, Blizzard Entertainment, Inc. v. Lilith Games (Shanghai) Co. Ltd. In that case, a third-party modifier and one of the original contributors to DoTA, Lilith Games, infringed DoTA's copyrights to create a mobile game, DoTA Legends and Heroes Charge.[119] The defendant in that case was one of the original modifiers of DoTA and argued that its mobile games were separate works and not derivatives of the copyright protected DoTA, which was owned by Valve. Lilith Games argued that Valve had no rights to subsequent works derived from DoTA, i.e.,Lilith's mobile version, and moved for summary judgment. The court held that Valve had validly acquired the rights to DoTA from the original modifiers and "may recover for original expression that [the original modifiers] contributed to their versions of DotA and DotA Allstars, as well as original expression that Valve itself contributed to DotA 2."[120]

DoTA illustrates how complicated creating a successful modification and establishing rights can be. From its inception, Blizzard arguably encouraged and facilitated modifications when it licensed out DoTA to third parties. However, despite coming to a mutual agreement, where Blizzard retained the noncommercial rights to DoTA and Valve retained the commercial rights to the same game, it is unlikely that this was the outcome Blizzard wanted, given its opposition to Valve's application to trademark DoTA. In its opposition to the USPTO, Blizzard argued that allowing Valve to trademark DoTA would essentially be allowing Valve to appropriate Blizzard's goodwill, because DoTA was created from Warcraft III and had gained popularity and association with it for several years.[121] Blizzard further argued that allowing Valve to own the trademark would create a source of confusion for the same reason.[122]

Blizzard's provision of modification tools most likely created the environment that caused Blizzard to lose DoTA to Valve. One of the original developers of DoTA used the Warcraft III editing tool to create DoTA and made his creation available as open-source code. Subsequent modifiers built upon the modification, and Valve later acquired these creators. Ownership of the modification was further exacerbated in Blizzard Entertainment, Inc. v. Lilith Games (Shanghai) Co. Ltd., when one of the original creators, who had already sold his rights, tried to make a mobile DoTA game and reclaim the intellectual property that belonged to Valve. Blizzard has since updated its custom game acceptable use policy, which now reflects a conservative approach to modification. Blizzard's terms state that "ownership [of] custom games are and shall remain the sole and exclusive property of Blizzard."[123] This could possibly be a reflection of its success and loss of DoTA, or purely a preventative measure, edging further away from strong encouragement of third-party end-user modifications.

---

119 Blizzard Ent., Inc. v. Lilith Games (Shanghai) Co., No. 3:15-CV-04084-CRB, 2017 WL 2118342, at 8 (N.D. Cal. May 16, 2017).

120 Id. at 11.

121 Notice of Opposition (Valve., Corp. v. Blizzard Ent., Inc.) ESTTA441431 (TTAB 2011), https://ttabvue.uspto.gov/ttabvue/ttabvue-91202572-OPP-1.pdf

122 Id.

123 Blizzard Entertainment Inc. (n.d.). *Custom Game Acceptable Use Policy*. Retrieved March 1, 2022, from https://www.blizzard.com/en-us/legal/2749df07-2b53-4990-b75e-a7cb3610318b/custom-game-acceptable-use-policy

Conclusion

Modifiers should take into consideration the interests that courts weigh when potential copyright issues arise. The court must balance the interests of the copyright holder, who put their labor, time, and creativity into developing a work, with those of end users, who are the ultimate beneficiaries of the games. It is in the copyright holder's interest to protect their work from copyright infringement in order to allow them to reap the benefit of publishing their work on the market and protect their intellectual property in order to promote the creation of more works. On the other hand, there are the interests of third-party end users, who are the ultimate beneficiaries and may want to alter gameplay to better enjoy it, or to reverse engineer a work to create something entirely new that will also benefit the public.

References

1. Allamanis, M., Jackson-Flux, H., & Brockschmidt, M. (2021). Self-Supervised bug detection and repair. *NeurIPS*. 1–22.
2. Gans, A.W., Krause, C.F., & Speiser, S.M. (2022). *American law of torts*. Thomson Reuters.
3. Lindstrom, C.O. (2020). Mod money, mod problems: A critique of copyright restrictions on video game modifications and an evaluation of associated monetization regimes. *William & Mary Business Law Review 11*(3), 811–843.
4. Lutten, L.J., & Wilf, F.M. (2021). *Computer software: Protection, liability, law, forms.* Thomson Reuters.
5. Wallace, R. (2014). Modding: Amateur authorship and how the video game industry is actually getting it right. *Brigham Young University Law Review*, 2014(1), 219–256.

Information about the author:

Christie A. Lee — Juris Doctor (J.D.), Hastings College of the Law, University of California, San Francisco, California, United States of America.
christie.alani@uchastings.edu

Сведения об авторе:

Ли К.А. — Juris Doctor (J.D.), Юридический колледж Гастингс, Калифорнийский университет, Сан-Франциско, Калифорния, Соединенные Штаты Америки.
christie.alani@uchastings.edu

https://doi.org/10.38044/2686-9136-2022-3-4-32-70

ARTICLES

SMART CONTRACT DISPUTES AND PUBLIC POLICY IN THE ASEAN+6 REGION

Gabriel R. De En Goh

The College of Law
570, George Street, Sydney NSW, Australia, 2000

Abstract

Smart contracts provide some benefits, such as better facilitation for contracting parties to monitor performance of their obligation and reducing the cost spent monitoring the contract. However, it is critical to understand various limitations of this concept as well as many legal and public policy uncertainties around it. Given the non-existence of an "universal rule" that governs smart contracts, the issues vary from jurisdiction to jurisdiction. The article applies comparative legal method to analyse the legal regulation of smart contracts in ASEAN+6 countries as well as the leading jurisdictions in the sphere of implementing digital technologies in the economy. Due to public policy considerations, there are different scenarios of smart contract development. The possible outlook is that ASEAN+6 countries would not accept smart contract as contract, cryptocurrency as property, and/or enforcing foreign awards that relate to smart contract disputes and/or cryptocurrency. Another possible way out of the deadlock is to govern relations under smart contracts by the UNIDROIT Principles. However, if the parties do not opt for such a solution, the determination of the applicable law will be left to the relevant conflict-of-laws rules with all of the uncertainties. Therefore, the author suggests that supranational laws is the better path for avoiding uncertainties in smart-contractual relationships.

Keywords

Smart contract, cryptocurrency, digital currency, Bitcoin, virtual asset, crypto asset, token, private international law, conflict of laws, public policy

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	De En Goh, G. R. (2022). Smart contract disputes and public policy in the ASEAN+6 region. *Digital Law Journal*, *3*(4), 32–70. https://doi.org/10.38044/2686-9136-2022-3-4-32-70

Submitted: 14 Aug. 2022, accepted: 28 Oct. 2022, published: 31 Dec. 2022

СТАТЬИ

СПОРЫ ИЗ СМАРТ-КОНТРАКТОВ И ПУБЛИЧНЫЙ ПОРЯДОК СТРАН АСЕАН+6

Г. Р. Де Эн Го

Школа права
2000, Австралия, Сидней, Джордж-стрит, 570

Аннотация

Смарт-контракты обладают рядом преимуществ, в частности облегчение контроля за выполнением условий договора сторонами и снижение затрат на мониторинг исполнения обязательства. Однако крайне важно учитывать технологические возможности смарт-контрактов, а также случаи противоречия последствий применения норм публичному порядку. Отсутствие «универсальных норм», регулирующих смарт-контракты, создает сложности их правовой регламентации, которые варьируются в зависимости от юрисдикции. В статье на основе сравнительно-правового метода проведен анализ опыта регулирования смарт-контрактов и в странах АСЕАН+6, а также в необходимых случаях юрисдикций, занимающих ведущие позиции в области внедрения цифровых технологий в имущественный оборот. Ввиду различной интерпретации публичного порядка существует несколько вариантов применения смарт-контрактов. Один из возможных подходов к их регулированию заключается в том, что страны АСЕАН+6 не будут квалифицировать смарт-контракты в качестве договоров, криптовалюту в качестве имущества, приводить в исполнение решения иностранных судов по спорам, связанным со смарт-контрактами и (или) криптовалютой. Возможным выходом может стать применение к смарт-контрактам Принципов УНИДРУА. Однако, в случае если стороны не включают условие об их выборе в качестве применимого права в договор, право определяется посредством применения коллизионных норм, что создает известные сложности. По мнению автора, указанных неопределенностей можно избежать при наличии соответствующей регламентации на наднациональном уровне.

Ключевые слова

Смарт-контракт, криптовалюта, цифровая валюта, биткоин, виртуальный актив, криптоактив, токен, международное частное право, коллизионное право, публичный порядок

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Де Эн Го, Г. Р. (2022). Споры из смарт-контрактов и публичный порядок стран АСЕАН+6. *Цифровое право, 3*(4), 32–70. https://doi.org/10.38044/2686-9136-2022-3-4-32-70

Поступила: 14.08.2022, принята в печать: 28.10.2022, опубликована: 31.12.2022

> *A new technology called "smart contracts" has emerged. What makes these legal agreements innovative is that their execution is made automatic through the use of computers.*
>
> **Max Raskin**[1]

Introduction

In this day and age, smart contracts have provided some benefits, such as better facilitation for contracting parties to monitor the each other's performance inside the contract, verifying if and when a contract, or one of its conditions, has been completed, guaranteeing that only the details necessary for completion of the contract are revealed to both parties, saving time through self-enforcement, and reducing the cost spent policing the contract, among others (Szabo, 1996).

This has, no doubt, provided speed and efficiency in the business context, as smart contracts essentially do not rely on human intervention, and their implementation is guided and overseen by other basic units of data structure (i.e., nodes) in the blockchain network. Hence, once the contract is triggered, the scripted contract self- executes (Nzuva, 2019).

Despite the various benefits of implementing smart contracts already noted, it is also critical to be aware that smart contracts are associated with various limitations, and there is much legal and public policy uncertainty surrounding smart contracts that has led to disputes. Some of these limitations and uncertainties are: (a) technology often outpacing the law and regulatory framework (Kõlvart et.al., 2016), (b) immutability, (c) contractual secrecy, (d) security, (e) enforceability of smart contracts under contract law, (f) governing legal and jurisdiction issues, (g) the legal value of blockchain-based proof, (h) blockchain creation of assets, (i) decentralized autonomous organizations (DAOs), and (j) blockchain transfers of value.

The legal uncertainties related to smart contracts are:

(a) whether a smart contract is legally binding;
(b) unexpected performance issues caused by coding errors;
(c) broader problems of enforceability;
(d) uncertainty over legal jurisdiction and governing law;
(e) formation;
(f) modification;
(g) public policy considerations.

Given the non-existence of a 'universal rule' that governs smart contracts, the uncertainty raised above varies from jurisdiction to jurisdiction and will be discussed in detail.

Taking into account the legal uncertainty surrounding smart contracts, how will countries' courts apply public policy considerations when being asked to set aside an award (at the seat) or refuse to grant recognition and enforcement? On the one hand, it is well accepted that public policy is meant to be construed narrowly. However, Article V (2b) of the New York Convention provides that: "recognition and enforcement of an arbitral award may also be refused if the competent authority in the country where recognition and enforcement is sought finds that the recognition or enforcement of the award would be contrary to the public policy of that country",[2] where it is referring to national public policy in the sense that it is either at the court at the seat that a party is seeking

[1] Raskin, 2017.

[2] Article V(2)(b), New York Convention (NYCG) 1958.

to set aside an award, or the court in the territory of enforcement if a party is seeking to challenge enforcement. One example where public policy is interpreted widely is the case of *Ruling Yue 03 Min Te No 719 (26 April 2020)* ("the Shenzhen case").[3]

Another example would be the Indonesian court's adoption of a wider position in the case of *Bankers Trust v PT Mayora Indah Tbk* (2000)[4] and *Astro Nusantara Bvetal v PT Ayunda Primamitra* (2010),[5] which caused problems in enforceability and recognition of foreign awards. However, in recent years, Indonesia had adopted a mixed approach to cryptocurrencies such as Bitcoin, Ethereum, Dash Litecoin, and Ripple under the Commodity Futures Trading Regulatory Agency (known as Bappedti). So, is this good news with respect to the recognition of smart contracts and virtual assets?

Undoubtedly, most courts in arbitration friendly jurisdictions will adopt a narrow interpretation of public policy. Jurisdictions like Singapore, Malaysia, and in recent years India, have adopted a narrow interpretation of public policy. The high standard required to set aside an award on grounds of public policy in the case of *BVU v BVX [2019] SGHC 69*[6] is one example. So, should national public policy considerations be construed as and confined to those matters that are found to breach natural justice, fairness, and equality? In this dissertation, we will extensively explore the positions of various countries in interpreting public policy, particularly, Singapore, Hong Kong, Malaysia, Indonesia, India, and China.

Is there something about smart contracts that is going to cause a problem there? It might in some nations. What if a country doesn't recognise a smart contract as being a proper contract or takes the view that smart contracts do not adhere to the traditional principles of contract law. Then, it is going to say that public policy is an issue. And what about courts in jurisdictions that do not accept that virtual assets like cryptocurrency are property?

Therefore, should parties have smart contracts governed not by a specific country's laws, but by supranational law, or even by soft law principles, such as the UNIDROIT Principles of International Commercial Contracts? Whatever the choice, it incumbent on parties and the tribunal to understand where enforcement is likely.

In the end, the courts are going to face inherent conflicts, as there is a demand for a narrow interpretation for public policy, but at the same time, national laws in some countries have not taken into account smart contracts or the approach they take to cryptocurrency as virtual assets. Therefore, at the moment, one way forward might be for parties to say they do not want the law governing a particular contract to be tied to any particular jurisdiction, and, instead, have the option of choosing supranational law or UNIDROIT Principles to govern the contract.

Another possibility that would give parties room to manoeuvre is the adoption of a form of Ricardian contract, where the parties can have an encoded version, as well as a natural language version. This could help in countries that are less inclined to accept smart contracts as proper contracts. Therefore, this research will be generally relevant to legal practice, as smart contracts are likely to be used for AI concluded contracts, as well as those involving virtual assets.

---

3 *Ruling Yue 03 Min Te No 719 (26 April 2020)*

4 The Decision of the Supreme Court No. 02 K/Ex'r/Arb.Int/Pdt/2000. Some authors have discussed this case, among others, Mills, K. (2006). *Enforcement of arbitral awards in Indonesia & other issues of judicial involvement in arbitration*, TMD 4. https://www.transnational-dispute-management.com/article.asp?key=804

5 The Supreme Court Decision No. 01 K/Pdt.Sus/2010. Some authors have discussed this case, among others, Mills, 2006; Kristy & Jing, 2013.

6 *BVU v BVX [2019] SGHC 69*

Why there could be conflicts between resolving smart contract disputes and applying public policy in the ASEAN+6

In light of the ongoing debate as to the use of smart contract technologies to enhance the way business is conducted, public policy considerations surrounding such usage, and the challenges regarding the widespread adoption of smart contracts, it is important to understand how smart contracts can be used to do more than just improve the way business is conducted.

As observed by computer scientist and cryptographer Nick Szabo (1996), because of the existence of smart contracts, "new institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. He called these new contracts 'smart' because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises specified in digital form, including protocols within which the parties perform these promises."

Ideal as it sounds, based on Nick Szabo's observation, "innovative technology does not necessitate innovative jurisprudence, and traditional legal analysis can help craft simple rules as a framework for this complex phenomenon."[7] Therefore, there must be opportunities to develop sustainable laws and public policy for smart contracting. With respect to legal and public policy issues surrounding smart contracting, this may be limited by the regularity of cases in different jurisdictions and individual territorial public policy considerations emerging in the ASEAN+6 region. Hence, for the use of the smart contract to be further advanced, there is a need to reconcile the legal and public policy considerations surrounding it.

It is arguably true that legal principles and public policy are, indeed, an important part of the recognition and the enforceability of smart contracts. However, it is possible to find room for improvement in these areas by examining ways in which laws and public policy are developed in the ASEAN+6 region, given that, in practice, smart contracts are playing a more important and pivotal role in facilitating the exchange of nearly all goods and services in various industries.

Businesses across the globe, as well as researchers and practitioners, widely recognize the benefits of smart contracts' unique features with regard to automatic execution, transparency, and immutability in a blockchain environment.

Although it must also be acknowledged that there are natural language and coding issues, this research will focus on, explore, discuss, and contribute to issues related to the following main areas:

(a) The application of traditional principles of contract law to smart contracts

(b) Current Public Policy trends with respect to awarding cryptocurrency in an arbitration award

(c) Case law on the enforcement of smart contracts and/or enforcement against virtual assets (i.e., cryptocurrencies)

(d) Jurisdictional issues and challenges in terms of public policy and law, particularly in the ASEAN+6 region.

(e) The relevance of resolving smart contract disputes to legal practice and the real world.

(f) Concluding Observations.

It is arguably true that there are ongoing difficulties in many areas such as (a) broader problems in enforceability, (b) uncertainty over jurisdiction and governing law, (c) formation, (d) modification, and (e) public policy considerations. It is also worth mentioning that governments have an important

[7] *Compare* Easterbrook, 1996 (arguing that the best way to learn and craft the law of a particular field is to study general rules), *with* Lessig, 1996 (arguing that the nature of cyberspace is unique and can reveal general principles of law); *and* Epstein, 1995 (arguing that basic legal principles can and should govern a complex, industrial society).

role to play to harmonize standards within the ASEAN+6 region with regards to the reconciliation of smart contract disputes and public policy considerations.

There may be issues in getting the courts to assist in producing or preserving evidence and/or freezing of assets, as some courts may not recognize smart contracts as contracts. Apart from the recognition and enforceability of smart contracts, even when a party is successful in securing an award, court order, or interim measure, there might be issues with respect to the arbitrability and/or enforceability of the court judgment.

Can one apply traditional principles of contract law to smart contracts?

Determining the legal definition of a 'smart contract' has, indeed, been one of the most controversial issues. Some distinguish between smart contracts, smart contract code, and smart legal contracts (Blemus, 2018).[8] However, it has been posited that any evaluation of their legal status must be guided by the law applying to the underlying contract (Kaulartz & Heckmann, 2016; Spindler & Woebbeking, 2019).

In a legal sense, just as traditional contracts are encoded, the law applicable to smart contracts is decided according to general principles, which means that the question of whether a legal contract has been concluded is dependent on the applicable legal provisions, which may, for example, require certain formalities that may lead to differing assessments of smart contracts in different jurisdictions (Reusch & Weidner, 2018).

In order to determine whether a smart contract can give rise to a legally enforceable contract, consideration must be given to whether each of the requirements necessary for a legally binding contract is met. It should be noted that the initial stage of concluding a contractual agreement does not significantly differ between smart and traditional contracts because, before a smart contract is activated, the parties must agree to a set of terms that initiate the program.[9]

Unlike traditional contracts, in the world of smart contracts, acceptance comes through performance. One can say they will initiate a smart contract, but there is no smart contract until they do. A smart contract can be posted to a ledger as an offer, but the contract is not formed until some action is taken to initiate acceptance, such as transferring a certain sum of money to the code.

Just as there is bargained-for consideration in traditional contracts, there is consideration in smart contracts.[10] The courts believe that mutuality of obligation distinguishes a contract from a gift for which parties do not have the same rights of legal enforcement. That is one of the reasons for having the doctrine of consideration.

A component of contractual law regulates issues where the parties, as a matter of law, cannot vary in their contracts from the mandatory provision laid down by contract law. Certain legal principles, like offer, acceptance, consideration, intention to create a legal relationship, contractual intention, certainty, and completeness, are so fundamental to the regulation of economic activity that courts will not enforce otherwise valid contracts if these principles are not complied with. There are also limitations on the freedom of smart contracts.

---

[8] ISDA, & Linklaters. (2017, August 9). Whitepaper on smart contracts and distributed ledger — A legal perspective. *LegalTechBlog*. https://legal-tech.blog/smart-contracts-and-distributed-ledger-a-legal-perspective

[9] The pieces of property do not need to be tangible; software systems can be embedded with contractware.

[10] "Courts have held a promise traded for another promise to be enforceable for well over 400 years, since the early to mid-1500s. Courts currently say that a mutual (or reciprocal or bargained-for) promise constitutes consideration for a promise, causing it to be enforceable" (Ricks, 1999).

It was mentioned earlier that smart contracts are considered 'smart', as they are self-executing. And of course, depending on the type of execution, they are divided into two categories. In the first category are those whose precise execution is known at the time of creation and, in the second, are those smart contracts whose execution is linked to a certain but unknown event or condition that cannot be encoded at the moment of creation.

It is important to note that blockchain and the smart contracts stored on them are immutable (i.e., practicably impossible to change), as the code is distributed on the blockchain across a network and would require sufficient consensus of the network to alter. Hence, once a smart contract is executed, its execution cannot be reversed even though a new transaction could be made by the parties to effectively nullify the result of the execution.

Smart contracts are undeniably widely used commercially. However, in the case of code-only smart contracts, the code that is executed and the outcome it produces represent the only objective evidence of the terms agreed upon by the parties. This is in contrast to cases with traditional text-based contracts, where courts will examine the final written document that the parties have agreed to in order to determine whether the parties are in compliance or breach. With code-only smart contract cases, email exchanges between the parties discussing what functions the smart contract should execute, or oral discussions to this effect, would likely yield to the definitive lines of code as the determinative manifestation of the parties' intent, as courts have long emphasized that it is this final agreement that represents the mutual intent of the parties (i.e., *consensus ad idem*, which is known as "the meeting of minds").[11]

Given the above considerations, the question to ask would be, "Is a 'smart' contract a real contract?" For obvious reasons, in order for a 'smart' contract to be a real contract, it must fulfil all of the requirements for contractual formation discussed above.

It has been proposed that the initial stage of a contractual agreement is similar for smart contracts and conventional contracts because, before any contract-ware can operate, two parties must agree to some set of contractual terms (Raskin, 2017). Therefore, it is a relief to know that the rules pertaining to offer and acceptance will not, in essence, pose an obstacle to the recognition of smart contracts as legally binding, as offer and acceptance, as well as the conduct of the parties, are evaluated objectively.[12] Furthermore, when parties submit their private cryptographic keys to commit resources to a blockchain-based smart contract, that is proof of a commitment (Werbach & Cornell, 2017).

When an offeror posts a smart contract on the blockchain in binary computer code clearly stipulating the terms of the transaction, it will be held to constitute an offer as opposed to an invitation to treat.[13] And once the proposed smart contract is posted on the blockchain and has fulfilled the requirements of being an offer in terms of identification of the *essentialia negotii* of the contract, it is effectively an acceptance by the offeree, and acceptance can be fulfilled through conduct.

For example, the offeror can write a smart contract stating that, for 30 Ethereum, the offeror will transfer ownership of a bicycle, including the terms of the deal, and upload it to a blockchain along with a digital token representing the bicycle and gas, which is payment for uploading the contract. Hence, this constitutes an offer. Subsequently, an offeree who is willing to accept will upload the 30 Ethereum to the smart contract, which constitutes acceptance. The smart contract will then detect

---

11 Lipton, A., & Levi, S. (2018, May 26). An introduction to smart contracts and their potential and inherent limitations, *Harvard Law School Forum on Corporate Governance*. https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/

12 *Smit v Hughes* (1871) LR 6 QB 597, 607 (Blackburn J).

13 Cf *Partridge v Crittenden* [1968] 2 All ER 421; cf *Carlill v Carbolic Smoke Ball Co Ltd* [1892] 1 QB 296.

the upload of 30 Ethereum and automatically transfer it to the offeror's wallet, while, at the same time, transferring the token to the offeree who uploaded the 30 Ethereum. The offeror does not need to confirm that he received the 30 Ethereum, and the token for the bicycle is transferred without further verification or discretion of the offeror. Therefore, the acceptance can occur either by performance or by the authorization of transfer by putting in the special cryptographic key (i.e., password) (Jaccard, 2017; Szczerbowski, 2017).

Performance of the terms in a unilateral contact or a signature by inputting the personal cryptographic key can be a clear act of acceptance. Therefore, the rules on offer and acceptance will not pose fundamental problems for the formation of smart contracts, as the procedure for forming such agreements are in accord with the elements of offer and acceptance.[14]

A point to note about contract law's approach to 'automatic contracts' is that a contract is formed when coins are inserted into a machine, in the case of *Thornton v Shoe Lane Parking* (similarly to *Szabo*'s vending machine analogy), and the fact that the subsequent process occurs without human intervention does not preclude the formation of a contract.[15] This is reinforced by the *R (Software Solutions Partners Ltd) v HM Customs & Excise* case, where it was held that an "automatic medium for contract formation" can result in valid contracts.[16]

In most common legal jurisdictions, the existence of valid consideration represents a mandatory condition for any contract to be legally enforced. For a consideration to be valid, it must only be sufficient,[17] and not adequate. Hence, the value and equality of mutual exchange is legally irrelevant from the perspective of contract law formation. Therefore, it is arguably true that the consideration requirement can easily be satisfied in the case of smart contracts, as smart contracts entail an exchange of digital assets, as in the example provided above describing the sale of a bicycle for 30 Ethereum.

However, an interesting argument has been raised by *Webach* and *Cornell,* who pointed out that smart contracts do not contain an exchange of promises, as is usually the case in normal contracts, or a requirement for a valid consideration. Both *Webach* and *Cornell* observed that "If someone balances a pail of water on top of a door, he does not promise to drop water on whoever next opens the door. Rather, he has merely set up the mechanical process by which that will happen. In a similar way, a contract to transfer one Bitcoin upon such-and-such event occurring is not really a promise at all. It does not say 'I will pay you one Bitcoin if such-and-such happens', but rather something like 'You will be paid one Bitcoin if such-and-such happens'... the so-called '[smart] *contract*' is not an exchange of promises or commitments. Creation of a smart contract — while setting certain events in motion — does not commit any party do no anything. There's nothing being prospectively promised" (Werbach & Cornell, 2017).

While this observation is surely a departure from the realm of traditional contracts. that issue did prevent the authors from reaching the conclusion that smart contracts are nonetheless legally valid contracts. Another author (Savelyev, 2017) has raised an additional question as to whether a smart contract is really a contract, given that it does not contain any obligation. He concluded that it is probably more correct to say that the main consequence of the conclusion of a smart contract is not the appearance of 'obligations', but the result of a self-limitation of certain rights by technical means.

[14] This might as outlined already before be different for the other mentioned category of smart contract where the algorithms act as an 'artificial agent'.

[15] *Thornton v Shoe Lane Parking* [1978] 2 QB 163 (Lord Denning MR).

[16] *R (Software Solutions Partners Ltd) v HM Customs & Excise* [2007] EWHC 971, para. 67.

[17] Illustration case: *Chappel & Co Ltd v Nestlé Co Ltd* [1959] AC 87.

Furthermore, *Werbach* and *Cornell* also argued that, though such commitments might not constitute promises per se, smart contracts are indeed agreements that purport to alter the parties' rights and obligations, and that an agreement may still be considered a contract even if it leaves nothing to be done or performed. Therefore, if one argues that smart contracts do not constitute a 'promise', but more of a guarantee, and, thus, cannot be recognized as a real contract, this is an unrealistically ideal view of contract law. Some considerations, such as benefits, rights or detriment, loss or responsibility etc., will be conveyed under smart contracts, inducing a reciprocal promise, and, pragmatically, there will almost always be sufficient consideration (Werbach & Cornell, 2017).

Intention to create legal relations in a commercial relationship is presumed in common law, and this presumption must be disproved by a party claiming that there is no such intention. It could be argued that, for every smart contract entered into in a commercial setting, the intention to create a legal relationship will be presumed.[18] Another more nuanced view offered by *Savelyev* (2017) is that, by concluding a smart contract, the contracting parties have demonstrated the intention to use an alternative regulatory system instead of traditional contract law.

Therefore, he observed, there might not be a true intent to create a legal relationship. However, the author also admits that, if the result is factually the same in substance to the one regulated by 'traditional contracts', it can be argued that the nature of the relationship is the same.

Most common law lawyers know that, for a contract to be enforceable, parties need to have the capacity to enter into such contract. However, most of the other existing blockchain platforms, in fact, do not check for full legal capacity (e.g., Ethereum). Instead, in principle, anyone can open an account without having sufficient capacity to do so. As there are no means by which smart contracts can test for capacity, they can be entered into by minors, drunks, or any other incapacitated person. Hence, people lacking capacity to sign a contract in the real world could potentially do so on the blockchain platform.

On the other hand, if there was no capacity, the party could then legally invalidate the transfer of any asset ex post by filing a lawsuit claiming unjust enrichment or, technically, through a reverse transaction (Schrey & Thalhofer, 2017).[19] However, this may not be an ideal alternative because there are pseudonymous users with cryptographic strings of random letters and numbers. Hence, it may be difficult to identify who to sue. Additionally, a reverse transaction can only factually rewind the contract, but not legally void the transaction, as it may remain on the blockchain since the blocks are immutable (Schrey & Thalhofer, 2017).

The above notwithstanding, the fundamental point remains that if a person possesses legal capacity, they will be free to enter into legally binding smart contracts. Last but not least, the contracting parties to a smart contract are technically not even people but only private cryptographic keys which represent individual people (Werbach & Cornell, 2017). Therefore, the question arises as to whether the issue of capacity can even be discussed since the parties are technically not human. It has been proposed that this is not a consideration for autonomous contracts, as the private keys do not act by themselves, but are instructed by humans.

Therefore, it is possible to believe that, by virtue of their flexibility, adaptability, and process of formation, smart contracts can be considered legally valid contracts, at least according to English contract law. Up to this point, it has been established that smart contracts can, in principle, fulfil the requirements for forming contracts.

---

[18] See e.g. *Esso Petroleum Limited v Commisioners of Customs and Excise* [1975] UKHL 4

[19] See also Jünemann, M., & Kast, A. (2017, May 1). *Rechtsfragen beim Einsatz der Blockchain* [Legal issues arising from the use of blockchain]. Kreditwesen. https://www.kreditwesen.de/kreditwesen/themenschwerpunkte/aufsaetze/rechtsfragen-beim-einsatz-blockchain-id40674.html

However, in the absence of a traditional governing contract, if there are mistakes in the code, a court reviewing a smart contract in a dispute faces difficulty in establishing any evidence as to what the parties had agreed upon other than the incorrectly encoded smart contract. Therefore, the incorrect code may be deemed to represent the understanding of the parties. So, in a smart contract dispute, courts may find it difficult to establish the parties' intention, which can be called a 'meeting of minds' between the parties.

It is well established in common law that the 'meeting of minds' element is important to contract formation, but, in French law, it is also essential to establish consent through a 'meeting of minds' (i.e. the *accord de volontes*) by identifying an offer by one party to do or not do something, as well as commensurate acceptance.[20]

The Singapore case of *Quoine Pte Ltd v B2C2 Ltd* [2020] deals with the two novel questions (a) what should be done when the contracting parties' algorithm operated as it was meant to in producing the resulting contract, but one party could, nevertheless, be said to have been labouring under a mistaken belief in entering into the contract, and (b) how should the law assess the state of the non-mistaken party in circumstances where no human is involved at the time of the formation of the contract?[21]

On the first issue, Quoine's central argument in its defence was that the contracts underlying the disputed trades (i.e., Trading Contracts) were invalidated in common law and in equity under unilateral mistake. Quoine also alleged that the Margin Traders entered into the contracts with B2C2 for buying and selling Bitcoin and Ethereum under the mistaken belief that they were transacting at prices that accurately represented or did not deviate significantly from the true market price, and B2C2 had actual or at least constructive knowledge of such a mistaken belief.

In order for Quoine to succeed in its claim on the first issue, it had to prove that: (a) in relation to unilateral mistake in common law, the relevant mistake must concern a fundamental term of the contract,[22] (b) B2C2 must either have actual knowledge (for unilateral mistake in common law) or constructive knowledge (for unilateral mistake in equity) of the mistake, and (c) in relation to unilateral mistake inequity, B2C2 was engaged in some unconscionable conduct in relation to the relevant mistake.

However, the Court of Appeals disagreed with the lower court's finding that the claimed mistake concerned the terms of the contract. Conscious that the price at which the Trading Contracts were brought by operation of the parties' respective algorithms and that these had operated exactly as they had been programmed to act, the mistake in this case was a mistaken presumption on the part of the Margin Traders as to how Quoine's platform would operate (i.e., the platform would not fail). Such a mistake was only a mistake in presumption as to the circumstances under which the Trading Contracts would be concluded, instead of a mistake as to the price at which the Trading Contracts were entered into.

With reference to the issue of knowledge, the majority of the Court of Appeals confirmed that, in the context of a deterministic algorithm,[23] it was the programmer's state of knowledge that was relevant to the parties. The relevant timeframe for assessing the programmer's knowledge was deemed

---

20 French Civil Code, arts 1101, 1106

21 *Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA(I) 02. Civil Appeal No 81 of 201.

22 The question of whether unilateral mistake in equity can extend beyond a mistake as to a term of the contract was not fully argued. The Court of Appeal was satisfied that it was not necessary to determine this question in this case.

23 A deterministic algorithm is one which always produces precisely the same output given the same input and does not have the capacity to develop its own responses to varying condition.

to be from the point of programming up to the point that the relevant contract was formed. This was supported by the view of *amicus curiae* Professor Goh Yihan, who recognised that the time of programming is when the programmer's knowledge is the most concretised.[24]

Programmers are not expected to be prophets and mistakes can take a wide range of forms. But it is clear that the law on unilateral mistake is concerned with (a) a type or class of mistake, that is one concerning the fundamental terms of the contract (at least in common law), and (b) the mental state of the non-mistaken party — whether they knew (or ought to have known) of the (type of) mistake and were acting to take advantage of it.[25]

However, "according to a paper published by the Association for Computing Machinery in 2016, coding bugs and other vulnerabilities were identified in nearly half of all smart contracts written on the Ethereum blockchain, potentially putting at risk $30 million worth of the virtual currency Ether. A review of Ethereum smart contracts conducted by Peter Vessenes, the co-founder of the Bitcoin Foundation, revealed at least 100 errors per 1,000 lines of code. The high error rate, in part, may be attributed to the fact that writing smart contract code remains highly complex. Researchers at the University of Maryland's cryptocurrency lab observe that 'even for very simple smart contracts (e.g., a Rock, Paper, Scissors game), designing and implementing them correctly was highly non-trivial.'"[26]

These high error rates may result in a surge in disputes relating to smart contracts. Although there are not many case authorities or materials that can be found regarding smart contract disputes, the case of *Quoine Pte Ltd v B2C2 Ltd* has provided some guidance on how smart contract disputes can potentially be resolved within the framework developed by the Singapore Court of Appeals. "It also enables the court to examine and consider the knowledge actually acquired after the point of programming and the actual conduct of the parties up to the time of the contract." However, the court emphasised that this is directed at *actual* conduct. The court also said that "rather, working backwards from the output that emanated from the programs, we are driven to assess the relevant state of knowledge by examining that of *the programmers*."[27]

Challenges surrounding encoded contracts vs natural language contracts

Natural language contracts (i.e., traditional contracts) have generally been the result of a reasonable arrangement between parties with break even with haggling control, i.e., parties arranging at arm's length (Savelyev, 2017). However, the very viability of smart contracts depends on the ability to express contractual obligations in code. For obvious reasons, natural language cannot be directly executed by a computer, and self-enforcement requires that the terms of the smart contract be computer-readable.

Therefore, there are multiple options: (a) a smart contract can be a translation of an existing agreement, it can be created in code from the outset or, (b) a contract can be drafted in natural language with subsequent encoding in mind. In addition, there are challenges associated with converting natural language into code and, more broadly, with encoding contractual obligations (i.e., 'encoding' of obligations).

---

24 *Quione, supra* note 1 at para 99.

25 *Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA(I) 02.

26 Potter, Anderson & Corroon LLP. (2018, February 7). *O'Toole, Kelly, and Hahn discuss why smart contracts need smart corporate lawyers.* https://www.potteranderson.com/newsroom-publications-OToole-Kelly-Hahn-Discuss-Why-Smart-Contracts-Need-Smart-Corporate-Lawyers.html

27 *Quione, supra* note 1 at para 98.

It is important to note two points before moving forward. First, it must be noted that the present discussion would not be relevant if technical writing restricted smart contracts to a very narrow range of relationships, whose performance was easily determinable by fixed formulae, as is the case with current smart contracts (Kiviat, 2015; Schroeder, 2016; Fairfield, 2015). In spite of the increasing recognition that some contracts cannot or should not be smart, many writings continue to extol the power of smart contracts to transform all types of contracts, including employment contracts, leases, and mortgages. As a second point, technical writings offer little guidance regarding how smart contracts should be formed or negotiated. The parties are generally assumed to create their own smart contracts or agree to use ones already created by somebody else.

Although smart contracts can be created as one-off, customized programs, economies of scale require that they be made into generic programs that can be used on a mass scale. These forms can include, for example, popular standard form agreements, such as those used for mortgages, car loans, and interest rate swaps.

In such a case, only certain values would be customizable for each transaction. The important thing to bear in mind is that it is likely that the smart contract will not be encoded by the parties themselves, or that at least one of the parties will not participate in its creation. As a result, either both of the parties or one of them will be unable to verify that the code accurately reflects their consent or how the smart contract works in practice.

That will inevitably lead us to the issue of contract translation. Because smart contract makers (i.e., coders) cannot decide on its business and legal aspects (Frantz & Nowostawski, 2016), it is reasonable to believe that there must be a document describing the substance of the agreement. Therefore, many smart contracts come from documents written in natural language that require further translation into code.

It has to be said that the complexity of this process is generally underemphasized, as technical writings extol consistent progress in the areas of machine learning and natural language processing and assume that the translation of natural language into code can be automated, or at least significantly facilitated by technological means. At the push of a button, agreements could be transformed into executable code, like source code is incorporated into object code. Notwithstanding predictable advancement in said areas, as of now, it is difficult to automate the transformation of natural language into code without a critical trade off in the nature of the yield of such transformation.[28]

Approximations appear to be admissible in mechanized interpretations of natural language, where the general importance of a sentence can be gathered from unique circumstances. These are nonetheless painful with respect to legal arrangements, which are drafted with fastidious exactness, where one single word may bring about accidental business outcomes and prolonged disputes.[29] Besides, accuracy appears to be vital when the smart contract is to self-execute and cannot be halted or revised. In the event that a smart contract is to embody a current arrangement, its interpretation into code will include a monotonous manual process, and developers fail to appreciate the low tolerance for mistakes in legal documents (Katz, 2013).

Additionally, developers appear to see contracts as sets of conditional statements abundant in standard clauses that can be unendingly reutilized for different transactions. While it is true that lawyers often rely on contractual precedents and (sometimes too eagerly) copy-and-paste individual provisions, it must not be forgotten that the standardization of legal language does not imply that such language is capable of reduction into an algorithm. Notwithstanding its formalistic nature,

[28] For a non-technical explanation of machine learning see Surden, 2014.

[29] On the limits of Natural Language Processing see Dale, 2010.

legal text is still natural language, and natural language is innately ambiguous, as the significance of words consistently relies upon context.

Hence, because of its long sentences, clauses, nested expressions, and references to abstract concepts, legal language is more difficult to translate into code than normal natural language. It has generally been suggested that smart contracts need to create a custom domain-specific programming language to capture the nuances of legal text.[30]

However, the main problem is that translating natural language into code is not the simple process of converting legal prose into computer-readable instructions but requires an interpretation of legal prose in advance. Interpretation is not an academic activity but is used to determine the exact scope of the obligations of both parties, the results to be achieved according to the contract, or the degree of effort required to perform specific obligations.

It is worth mentioning that the successful performance of a contract may depend on the meaning of a word, and disputes over a word may lead to lengthy litigation. There is hardly a contract that does not require some interpretation, thus, the presence of some legal and commercial knowledge on the side of the interpreter is necessary. Hence, in the case of a smart contract, this would have to be performed before, or in parallel with, the process of translating the legal text in code. However, developers can hardly be expected to perform this task.

Interpreting contracts requires in-depth knowledge of the principles governing contractual interpretation (i.e., principles surrounded by multiple controversies relating to the question of *how* to determine objective meaning of words and expressions, or the meaning that must be *deemed to have been intended by both parties)*. This meaning may depend on other words used in a given contractual document, or more broadly, on the context in which they are used.[31] Whoever interprets a contract must be able to decide between the literal and the purposive approach and, in the event of competing interpretations, select the one that is more consistent with business common sense.[32]

This would mean that the interpreting developer would have to ascertain the meaning that the contract "would convey to a reasonable person having all the knowledge which would reasonably have been available to the parties in the situation in which they were at the time of the contract."[33] Furthermore, it should not be forgotten that the interpretation process is not limited to the case in which words are ambiguous and can sometimes also reveal the existence of ambiguities.[34]

For contracts in natural language, it may not be immediately evident to the parties that a particular word or expression may have multiple interpretations. However, in the smart contract context, the issue would not lie with the parties disagreeing over the meaning of the words, but in the likelihood that those deciding how to covert a particular obligation into code will make a mistake in interpretation. It should be noted that most contracts contain gaps which require that terms be implied to make the agreement workable in practice. Contractual interpretation is usually performed by courts after a dispute has arisen, and the implication of terms is traditionally determined by courts, and not contracting parties.

If the implication of terms requires an understanding of legal rules, as well as the commercial context of a particular transaction, coders may not be able to identify and fill contractual gaps

30 See e.g. Wolfram, S. (2016, October 12). Computational law, symbolic discourse and the AI constitution. *Stephen Wolfram Writings*. https://writings.stephenwolfram.com/2016/10/computational-law-symbolic-discourse-and-the-ai-constitution/

31 Coote, 1988.

32 *Rainy Sky SA v Kookmin Bank* [2011] UKSC 50; *Re Sigma Finance Corp* [2009] UKSC 2.

33 *Hombourg Houtimport BV v Agrosin Private Ltd (The Starsin)* [2003] UKHL 12.

34 *Napier Park European credit opportunities fund ltd v Harbourmaster Pro-Rata CLO BV* [2014] EWCA Civ 984.

themselves. For instance, there is no flexibility for parties to incorporate a term that has one meaning at the time of execution but can be interpreted differently during the performance phase. Therefore, what can be done when the meaning of terms needed in a smart contract can vary?

Variation of terms and how it is done?

Although arguments may be presented that the problems surrounding the interpretation of supplementary contractual language may be solved by lawyers and coders collaborating to translate legal documents into executable code, it must be noted that, in spite of such collaboration, neither the parties nor their lawyers will be able to ascertain whether the code in the smart contract correctly reflects the originating legal documents. For example, even if a smart contract mirrors this document, with all its nuances, there is still potential for inconsistencies between what was agreed upon and what was implemented. Such inconsistencies are particularly confusing given that, once a smart contract commences self-enforcement, it cannot be stopped or amended.

It must be said that, at present, there is no simple path to amend a smart contract that would create certain challenges for contracting parties. Amendments or modifications are relatively easy in conventional contracts, and parties can waive provisions if they so choose. However, smart contracts lack flexibility in semantics and enforcement, when compared to conventional contracts. Hypothetically speaking, with a traditional text-based contract, if there was a change in law, the parties could quickly draft an amendment to address that change, or alter their course of conduct. Smart contracts do not currently offer such flexibility. It is worth mentioning that, given that blockchains are immutable, modifying a smart contract is far more complicated than modifying standard software code that does not reside on a blockchain.

Given the current technical and economic uncertainty of this phenomenon, the debate over its legal implications is equally precarious, and defending the idea of disseminating these technologies requires some sort of a leap of faith. On the one hand, true believers in smart contracts and blockchain magnify these tools, their potential, and their capacity to bring the automation of contracts to its limits (Surden, 2012). They promote the use of technologies that can allegedly predict a huge number of variables to provide highly sophisticated solutions.[35] On the other hand, there are scholars who are unwilling to endorse this technological miracle. They express doubt about the capacity of smart contracts to embrace all the different facets that characterize traditional contracts and their bargaining processes and, thus, suggest a more cautious approach (Druck, 2018; Levy, 2017).[36]

There is also a chance that amending a smart contract may produce higher transaction costs, as supposed to amending a text-based contract, and increase the possibility that the parties will not accurately reflect the modifications they intended. Similar challenges also exist with regard to terminating a smart contract, for example, if a party discovers an error in an agreement that gives the counterparty more rights than intended, or concludes that fulfilling its stated obligations will be far more costly than expected. In a text-based contract, a party can engage in, or threaten, so-called 'efficient breach' (i.e., knowingly breaching a contract and paying the resulting damages if it determines that the cost of performing is greater than the damages it would owe). By ceasing performance or threatening to take that step, a party may bring the counterparty back to the table to negotiate an amicable resolution. Smart contracts do not yet offer analogous self-help remedies.

---

35 Buterin, V. (2014). A next generation smart contract and decentralized application platform. *Ethereum White Paper*. https://github.com/ethereum/wiki/wiki/White-Paper

36 Schumpeter. (2016, July 28). *Not-so-clever contracts.* The Economist. https://www.economist.com/business/2016/07/28/not-so-clever-contracts

Hence, can variation of terms be done before concluding a contract? This consideration has two consequences: on the one hand, it invites scholars to address the divide between unilateral and bilateral contracts and its implication within the realm of smart contracts. On the other hand, and more importantly, it reveals that the traditional narrative that smart contracts can serve as tools to reduce time and transaction costs might be superficial as soon as the creation of a (true) smart contract requires the contribution of a plurality of people. Someone who wants to launch a contractual initiative needs, first and foremost, a software developer (Walch, 2018) to transpose the instructions related to the various aspects of the agreement into virtual architecture, to build a data model (structured according to directives and conditionals) for the offer to operate, while also taking into consideration the different forms of interaction between the counterparties. Hence, it may be said that the possibility of completely eliminating the role of an intermediary is already confuted at its roots.

Moreover, consider also that the developer must also be able to communicate with another operator who is in charge of establishing the conditions for access to the platform where the code will operate (and where the general public, or the counterparty, will be able to find and eventually conclude it). Finally, users acting on the platform must be able to interact with the 'offer' if they wish to amend its conditions before concluding the contract, as traditionally happens during negotiations. This requires the presence of other intermediaries on their side as well.[37]

This would imply that, without the development of mechanisms that allow contracting parties to address a change in circumstances and more easily adjust terms, the utility of stand-alone smart contracts that were intended to have legal effect may be limited, particularly in complex transactions. In these circumstances, the necessary flexibility and management of contract amendments may be provided by augmenting smart contracts with a master agreement, a conventional (natural language) contract, or an overarching participation or governance framework having legally binding effect.

Given the practical impossibility of amending terms in smart contract, as the code is distributed on the blockchain across a network and would require sufficient consensus of the network to alter, the only solution for creating the effect of amending a blockchain smart contract is to deploy and use a new one instead. Therefore, could a Ricardian contract model that links smart contracts to traditional contracts solve the issue of amending contractual terms? As commercial transactions are dynamic, this is left for the parties to decide. The question of whether a smart contract should be linked to a traditional contract will be largely dependent on the complexity of the deal.

Smart contracts can help facilitate safe and transparent transactions, whose records are immutable, while traditional contracts and legal institutions can ensure their validity, provide the required legal framework, and take care of disputes. This means that the Ricardian contract will consist of both a smart contract and a legal contract (i.e., traditional/natural language contract), where the legal contract is supplemented and not replaced. Therefore, to handle complex legal issues, it is possible to suggest that, until there is greater clarity on standalone smart contracts, parties should consider using Ricardian contracts (smart contracts that are governed by or which implement provisions of a traditional contract) with a traditional contract they know a court will enforce.

[37] A thoughtful investigation of this topic has been offered by Cohney, et al. 2019, who investigated a series of 50 2017 'Initial Coin Offerings', ICOs, conducted on smart contracts. Despite the offering claim that "code does have the potential to become a substitute and complement for old-fashioned legal governance in financial contracting", the Authors ultimately observed that "potential does not mean reality. Our study shows just how far code falls short of expectations".

Encoded Contracts vs Ricardian Contracts vs Traditional Contracts

Having extensively discussed and explored the issues pertaining to encoded contracts vs natural language contracts in the previous sections, we have come to the topic of Ricardian contracts. It is worth reiterating that smart contracts are automated applications that run on blockchain technology, without third-party enforcement or verification. They are designed to result in a particular agreed-upon outcome based on a set of if- then premises that put actions into motion once certain conditions are met. Because the blockchain records information in a manner that can be described as immutable, the execution of smart contracts is often irrevocable, which means that, once a certain action is in motion, it cannot be undone.[38] It is also worth mentioning that both smart contracts and Ricardian contracts need to satisfy all of the requirements of a legally binding contract to be enforceable.

Since smart contracts are written in code, it is difficult to determine and enforce the agreement if there is no natural language contract that sets out the terms, especially in circumstances where the code contains an error or carries out an action contrary to the parties' intentions. Furthermore, it is unclear whether the if-then statements embodied in the computer code will necessarily meet all of the requirements of a contract.

A Ricardian Contract is a legal contract that was first introduced in 1995 by a well-known programmer, Ian Grigg, and this concept is now part of the blockchain. What makes Ricardian contracts unique is that they are cryptographically signed and verified. As opposed to encoded contracts, Ricardian contracts are available in a human-readable text that is easy to understand (not only lawyers), and these legal agreements or documents can be read by both computer programs and humans.

To put it simply, they serve two purposes. Firstly, they are easy-to-read legal contracts between two or more parties that lawyers can easily understand. Secondly, they are machine-readable. Hence, Ricardian contracts can be easily hashed, signed, and saved on the blockchain. On the whole, Ricardian contracts merge legal contracts with blockchain technology and bind the parties by a legal agreement before the execution of the actions on the blockchain network.[39]

Ricardian contracts set out the intentions, as well as actions that will take place in future based on a legal agreement. The foundational difference between Ricardian contracts and smart contracts on blockchain platforms is the type of agreement. The difference is that Ricardian contracts record an agreement between multiple parties, while smart contracts execute whatever is defined in the agreement as actions. Refer to the table comparing Encoded Contracts vs Ricardian Contracts vs Traditional Contracts below.

So, do Ricardian contracts provide more clarity and certainty with respect to the terms of the contract? These issues may be addressed by Ricardian contracts that link a natural language contract to the underlying code. Since the text clearly specifies the smart contract code with which it is associated, the parties can clearly see the variables that are passed on to the smart contract, as well as how they are defined and how transaction events will trigger the execution of the code.[40]

The characteristics of Ricardian contract can be summarized as follow[41]:

---

38 Lim, C., Saw, T. J., & Sargeant, C. (2016, July 28). Smart contract: Bridging gap between expectation and reality. *Law Faculty website.* https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality

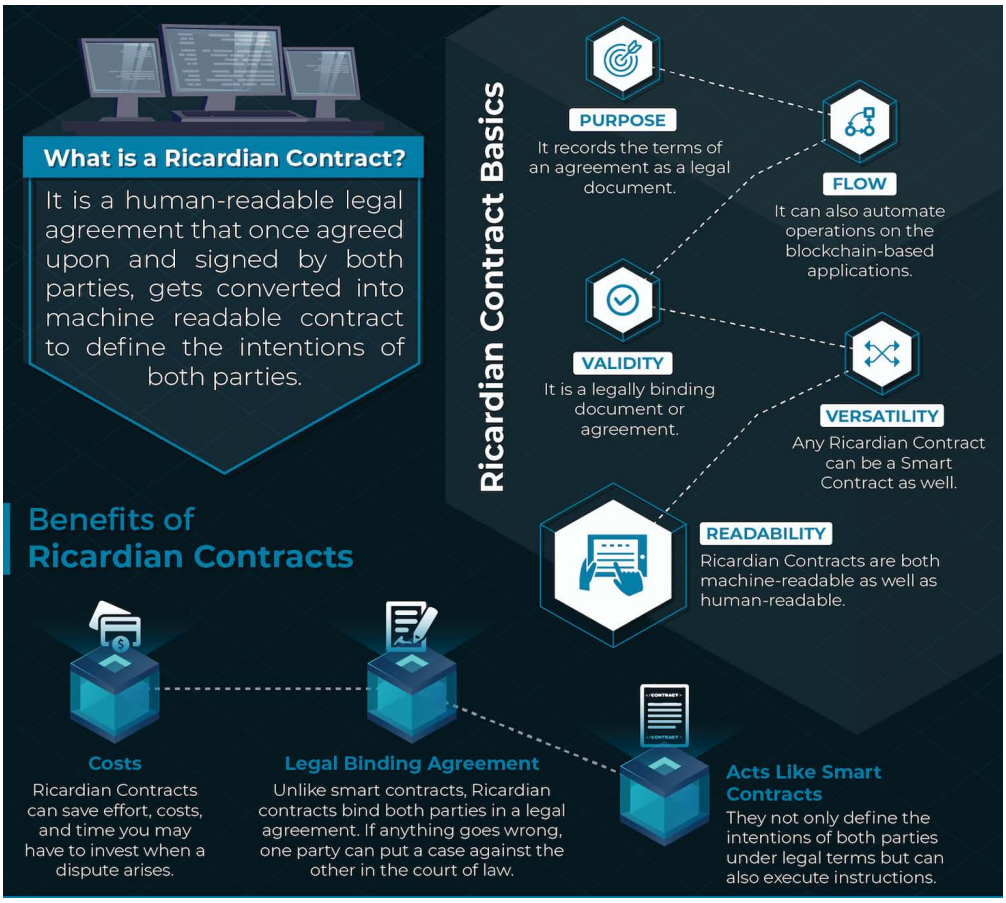
39 Geroni, D. (2021, 14 September). What are Ricardian contracts? A comprehensive guide. *101 Blockchains*. https://101blockchains.com/ricardian-contracts/

40 Lipton & Levi, 2018.

41 Grigg, I. (n.d.). Guide to Ricardian contracts. *WebFunds*. http://www.webfunds.org/guide/ricardian.html

Figure 1

Overview of How Ricardian Contracts Work[42]



Note. Created by author.

1. Human parsable;
2. Printable document;
3. Program parsable;
4. All versions (i.e., displayed, printed, parsed) are manifestly equivalent;
5. Signature of the Issuer;
6. All relevant information is present in one single document, including signature and parties. This, along with the *manifestly equivalent* characteristic above, results into the *Rule of One Contract*;
7. It can be represented as a legal contract;
8. It can be identified securely, wherein 'securely' means any attempt to distort the linkage between a reference and the contract is not feasible;
9. It is supported by financially capable PKI (such as OpenPGP (https://www.openpgp.org/));

[42] Geroni, 2021.

Figure 2

Comparison Table: Smart Contracts vs Ricardian Contracts vs Traditional Contracts

Characteristics	Smart Contract	Ricardian Contract	Traditional Contract
Purpose	- Execute the Terms of an agreement - Self-executing of the contract	- Execute the Terms of an agreement - Capable of self-executing - Record the terms of the agreement in human readable form as a legal document	- Execute the Terms of an agreement - Record the terms of the agreement in human readable form as a legal document
Flow	Automate actions on the blockchain-based applications	It can also automate operations on the blockchain-based application	There is no automation involved
Validity	To legal binding contract for smart contract	To legal binding contract for smart contract	To legal binding contract for smart contract
Versatility	Cannot be Ricardian Contract	Any Ricardian contract can be a smart contract as well	Can be converted into Ricardian Contract for the human readable contract layer
Readability	Smart contract are machine-readable but not necessarily human-readable	Ricardian are both machine and human readable	Only human readable

Note. Created by author.

10. Extensible — it can interpret bonds, shares, loyalty, etc.;
11. It can identify the legal issuer (signer of contract) and issuance server;
12. Cannot be changed by anyone except a legal issuer or other parties to the contract;
13. Verifiable in nature; and
14. Permissionless — the contract can be created and used by anyone without requiring allocations in controlled spaces.[43]

It is worth highlighting some other benefits of Ricardian contracts. First of all, they are secure in nature, as they use hidden signatures, and the signing of contracts takes place through private keys. Later, the hash of the agreement is used to attach that hidden signature to the contract. Ricardian contracts also offer protection to parties in an agreement who do not have equal bargaining power from parties in a stronger position that may be more likely to unilaterally change the terms of the agreement during execution. Hence, once the agreement is finalized, it cannot be unilaterally modified, making it very secure. Furthermore, when the signature of the issuer is added to the contract, it creates a legible and binding agreement with respect to the information described in the document. This also makes it possible to track the parties involved with the help of a private key and hold them accountable.[44] Therefore, it has been suggested that Ricardian contracts may be the best way to bridge the gap between law and technology today.

[43] Grigg, n.d.
[44] Geroni, 2021

Is Cryptocurrency Property?

United States

At the outset, it must be said that this discussion on whether cryptocurrency can be considered property, and its regulatory treatment in various jurisdictions, is based on the positions that the jurisdictions have adopted at the time of this paper was written.

If smart contracts, in principle, are capable of fulfilling the requirements for the formation of contracts, then the natural question that follows would be, "Can virtual assets be seen as property?" However, in order to answer this pressing and controversial question, it is necessary to explore and examine the approach to crypto assets in property law, as well as its regulatory status.

In recent years, it has been noticed that most jurisdictions (like US, UK, Australia, Singapore, and Hong Kong) have begun to edge their way towards formally recognizing this new category of property, despite the fact that crypto assets do not generally fall within the traditional criteria for property — with the exception of tax authorities, which moved in this direction early in order to protect the tax base.

As crypto assets become more important in the economy, more governments around the world have realized that crypto assets are property. This recognition has been based on a gradual expansion of related principles and a lot of pragmatism. The classification of crypto assets into value/asset, payment, or utility tokens has been widely adopted and follows the regulatory consequences. However, the difference lies in how each regulator analyses a token taking into account the terms of their country's securities and payment laws.

For example, in the United States, cryptocurrencies are subject to different and sometimes overlapping legal and regulatory systems. These systems may include currency, securities, commodities, or general intangibles, as it depends on the specific circumstances considered by the investigation. Although it is not yet an established law, cryptocurrency is considered personal property in various situations. The US Supreme Court has well established that property rights are a creature of state law. Property rights are not empowered by the federal constitution, rather, "individual entitlement [to property] is grounded in state law."[45]

However, at a statutory level, the State of Wyoming recently enacted a law that came into effect on July 1, 2019, which explicitly recognizes digital assets (including cryptocurrency) as intangible personal property.[46] In most states, it remains arguable whether cryptocurrencies meet the criteria established by the courts for the recognition of a property interest. In reference to a dispute over property rights concerning Supplemental Type Certificates issued by the Federal Aviation Administration, the Ninth Circuit Court of Appeals identified three criteria under California law: (i) an interest capable of precise definition; (ii) capable of exclusive possession or control; and (iii) where the claimant has established a legitimate claim to exclusivity.[47]

Therefore, the regulatory perimeter can be found in IRS Notice 2014-21, 2014-16 IRB 938 (14 April 2014), where the Internal Revenue Service ruled that, for federal tax purposes, cryptocurrencies are treated as property.[48] Some other agencies also place cryptocurrencies in the 'digital assets' category. For example, on November 16, 2018, the US Securities and Exchange Commission (SEC) issued a Statement on Digital Asset Securities Issuance and Trading, and, on April 3, 2019, issued a Framework

[45] Logan v. Zimmerman Brush Co., 455 U.S. 422, 430 (1982).

[46] W.S. SF0125

[47] G.s. Rasmussen & Associates, Inc. v. Kalitta Flying Service, Inc., 958 F.2d 896 (9th Cir. 1992).

[48] I.R.S. Notice 2014-21, 2014-16 I.R.B. 938 (14 April 2014).

for Investment Contract Analysis of Digital Assets. Both directions from the SEC use the term "digital assets" when referring to cryptocurrencies.

United Kingdom

The status of cryptocurrencies, distributed ledger technology (DLT), and smart contracts is still unclear under both English private and financial regulation. Under English law, personal property is either a 'chose in possession' or a 'chose in action'. For example, English law does not expressly treat intangible Bitcoins based on DLT as either. Furthermore, data or information is not considered property in itself, nor do Bitcoins create contractual rights against anyone, though it is said by HM Revenue & Customs that crypto assets are property for the purpose of inheritance tax.

However, it is worth noting that in the July 2019 case of Robertson v Persons (unreported, CL-2019-000444) the London Commercial Court indirectly 'recognized' Bitcoin as legal property for a time. This is because the court is preparing a temporary asset preservation order to prevent stolen Bitcoins from disappearing or being transferring in cases of hacking, when email accounts are attacked by spear phishing. The attackers transferred most of the Bitcoins to a digital wallet leading back to the UK subsidiary of a well-known digital currency exchange. Some have argued that the 'theft' of Bitcoin did not transfer ownership to the hackers, so ownership cannot be transferred to exchanges. However, the judge recognized and accepted that this was a question to be tried.

Interestingly, the claimant relied on a decision by Simon Thorley IJ in the Singapore International Commercial Court case of B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(I) 03, where Bitcoin was held to be personal property that can be the subject of a trust. In addition, an English High Court decision in Armstrong DLW GmbH v Winnington Networks Ltd [2012] EWHC 10 (Ch)[49] was referred to, which concerned the fraudulent transfer of carbon emissions allowances, where the court upheld the claimant's claim for the value of the allowances on the basis that they constituted a form of intangible property.

While there is still uncertainty over crypto assets and smart contracts in the UK, the regulatory treatment by the Financial Conduct Authority (FCA) suggests that their categorization depends on their intrinsic structure, as well as their purpose. Security tokens that grant ownership rights, refund specific amounts, or share future earnings are considered "specific investments" under the UK Regulatory Activities Order and possible "transferable securities" under the EU Market in Financial Instruments Directive. Such crypto assets fall within the scope of financial supervision and are therefore also within the scope of the FCA's powers, as well as investment products, such as derivative contracts that reference these crypto assets. The FCA proposes that retail sales of these be banned. Other tokens that meet the definition of e-money under the Electronic Money Regulations are also fall within regulation.

But it is worth noting that redeemable utility tokens for specific products or services, which are usually provided using DLT platforms, would fall outside of regulation. That would mean that cryptocurrencies, crypto-coins, or payment tokens such as Bitcoin and Litecoin could potentially fall outside of regulation. In comparison, stable-coin cryptocurrencies that are linked to fiat currencies would possibly constitute e-money. At the very least, the FCA published guidance has the merit of setting out its approach to the regulatory treatment of crypto assets. At the very least, as of now, crypto assets would be brought within the AML/CTF regime in accordance with the recommendations of the Financial Action Task Force when the UK passes the EU's Fifth Money Laundering Directive into national law.

[49] Armstrong DLW GmbH v Winnington Networks Ltd [2012] EWHC 10 (Ch).

Australia

Although commentators have noted that, in considering Australia's general law and economic test for property, it is likely that crypto assets like Bitcoin would amount to property. However, to date, there has been little guidance as to whether a crypto asset would be recognized as property under Australian law. Property is usually considered in the context of "rights to identifiable things." In practice, when something does not meet the accepted indicia for property, the definition does not standstill and the indicia adapts so that the "thing" is not improperly excluded.

Looking through the lens of regulatory treatment of crypto assets in Australia, the Australian Treasury launched a public consultation on initial coin offerings (ICOs) in February of 2019 and called upon industry stakeholders to make submissions. The issues paper published in conjunction with the consultation considers Australia's current regulatory framework for crypto assets and asks if further regulatory action is needed to address the risks posed by ICOs and promote the smooth functioning of the Australian ICO market.

In 2019, both the Australian Securities and Investments Commission's (ASIC) information sheet on ICOs and crypto assets (INFO 225) was revised. This provides guidance on how the Corporations Act 2001 may apply to crypto assets. Under the said Corporations Act 2001, persons dealing in financial products must hold an Australian financial services licence. Importantly, ASIC noted that each crypto asset will be evaluated individually based on the specific rights and characteristics of the crypto asset.

While there have been legislative amendments to accommodate the use of cryptocurrencies, these have principally focused on transactional relationships (for example, the issuing and exchanging process) and activities involving cryptocurrencies rather than the cryptocurrencies themselves.

The four most common characterizations of crypto assets are as follow, and each requires the person dealing in these crypto assets to hold a licence and comply with ongoing obligations:[50]

- Interests in a managed investment scheme (MIS) have three elements: (i) the contributions of money or assets to obtain an interest in benefits produced by the scheme; (ii) those which are pooled or used in a common enterprise to produce financial benefits (or interests in property) for those who hold interests in the scheme (e.g., using the contributor's funds to build the platform); and (iii) that the contributors do not have day-to-day control over the operation of the scheme. In certain cases, an ICO might constitute a MIS and a crypto asset, therefore it could be an interest in an MIS.
- Securities: Under section 92 of the Corporations Act, securities include shares, debentures or units of shares. A crypto asset may constitute a share where the rights attaching are similar to those usually attached to a share. For example, where there is a right for the owner of the crypto asset to participate in the profits of the company, then the crypto asset may be a share.
- Derivatives: A crypto asset may be characterized as a derivative, where the value of the cryptocurrency is ultimately determined, derived from, or varies by reference to the value or amount of an external reference (e.g., an asset, rate, index or commodity). Asset-backed tokens that are backed by real world assets, such as oil, may in this way constitute a derivative.
- Non-cash payment facilities: A crypto asset may constitute a non-cash payment (NCP) facility under section 763D of the Corporations Act. A cryptocurrency would be an NCP where a person makes payments, or causes payments to be made, other than by physical delivery of cash. It is likely that several utility tokens used for the payment for goods and services would fall to be regulated as NCP facilities under Australian financial services law.

[50] Reeves, P., O'Grady, R., & Shen, E. (2022). Australia. In J. Dewey (Ed.) *Blockchain & cryptocurrency regulation 2023*. Global Legal Insights. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/australia

Singapore

There have been discussions in Singapore regarding the legal characteristics of Bitcoin and other crypto assets for the past five years. Yet is remains a difficult and debatable issue, which is complicated by the lack of a uniform definition for 'crypto assets' that can be applied to a broad class of instruments with different functionalities. However, there are developments worth noting that may provide some clarity in this space.

As discussed above, the decision on the very first Singapore case of B2C2 Ltd v Quoine Pte Ltd (B2C2) was referred to by the English Courts. Although this point is not technically disputed between the parties, this case is the first judicial reference to use the cryptocurrency as property. Although the decision referred to cryptocurrencies in general, there is increasing recognition that the nature and application of both Bitcoin and Ether differs from security tokens or utility tokens. Correspondingly, such cryptocurrencies would warrant different regulatory treatment.

Legally, Singapore offers a neutral regime for the growth of transactions involving cryptocurrency. Singapore law is commonly used as the governing law in cryptocurrency related contracts because of its advanced dispute resolution laws and its reputation for being an arbitral friendly and neutral regime.[51] The Payment Services Act (**PSA**) came into effect in January of 2020 to regulate traditional as well as cryptocurrency payments and exchanges. The intention behind introducing the PSA was to streamline payment services under a single piece of legislation and calibrate regulations according to the risks such activities pose by adopting a modular regulatory regime (Ho & Law, 2021). The PSA provides a framework to obtain a license to operate a cryptocurrency business in Singapore and outlines money laundering compliances to be met by cryptocurrency operators. The relevant provisions can be found as follows:

(1) Digital payments token: The PSA uses the term "digital payments token" to refer to virtual currencies and defines it as any digital representation of value that:

a. is expressed as a unit;

b. is not denominated in any currency, and is not pegged by its issuer to any currency;

c. is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of a debt;

d. can be transferred, stored or traded electronically; and

e. satisfies such other characteristics as MAS may prescribe.[52]

Digital Payments Tokens (DPT) recognized by MAS include Bitcoin and Ether. The PSA further recognizes a digital payment token service as dealing in digital payment tokens and facilitating the exchange of digital payment tokens.[53]

(2) License: Any person carrying out a digital payment token service must obtain a payment institution license, unless exemptions apply.[54] A standard payment institution license applies to companies with payment transactions up to $3 million per month and a major payment institution license must be obtained by companies with payment transactions which exceed $3 million per month. An application for both these licenses must be made by a company incorporated in Singapore or overseas, has its permanent place of business or registered office in Singapore; and has at least one

[51] So, A., & Tham, F. S. (2020, January 15). Singapore: Why Singapore has become Asia's cryptocurrency and blockchain hub. *Taylor Vinters.* https://www.mondaq.com/fin-tech/883798/why-singapore-has-become-asia39s-cryptocurrency-and-blockchain-hub

[52] Section 2, Payment Services Act, 2019.

[53] Part 3, First Schedule, Payment Services Act, 2019.

[54] Section 5 and 6, Payment Services Act, *supra* note 12.

executive director who is a Singapore citizen or a permanent resident or is a person belonging to a class of persons prescribed by the MAS.[55]

(3) Anti-money laundering (AML)/Countering the financing of terrorism (CFT): MAS has released a separate notice on AML/CFT guidelines for DPT service providers. As per the notice, DPT service providers are required to set up robust controls to detect and prefect money laundering and terrorism financing.[56] All DPT payment service providers must implement certain measures as a part of their internal AML/CFT policy, which includes:

a. customer due diligence by verifying their identities and businesses;

b. monitoring customer transactions for signs of money laundering and terrorism financing;

c. screening customers by comparing them against relevant UN international sanctions lists; and

d. maintaining detailed records of customer activities and putting in place a process to report suspicious transactions to MAS.[57]

Generally, persons dealing in crypto assets should be mindful of the implications of:

- the Commodity Trading Act (CTA);
- the Securities and Futures Act (SFA); and
- the Payment Services Act (PSA).

Among other classifications, a crypto asset may be:

- a commodity under the CTA;
- a capital markets product under the SFA; or
- a digital payment token (DPT) under the PSA.

A crypto asset, which is a digital representation of value that is expressed as a unit not denominated in or pegged to any currency and intended to be a medium of exchange, is likely to fall within the definition of a DPT. For example, this includes Bitcoin and Ethereum. Therefore, any business in Singapore that deals in DPTs or offers any service facilitating the exchange of DPTs is considered to perform a digital payment token service, which is a regulated activity under the PSA regime.

The regulator has not defined virtual currency (used interchangeably with 'cryptocurrency' or 'token' or 'coin', unless otherwise specified) to be one exclusive thing, but instead has stated the following:

(a) they are not a currency or legal tender issued by any government;

(b) they are to be encouraged as a means of paying for goods or services to someone who is willing to accept them as a mode of payment, and are a means of making payments;

(c) they cannot be a store of value, as their prices fluctuate (in this regard, the government attitude is not to encourage people to use them as an investment tool, as they are risky);

(d) they are recognised as assets and personal property, with more and more people trading in them.

Switzerland

There is an ongoing discussion about the legal status of crypto assets under Swiss private law. Possible classifications include movable property, energy rights recognized by civil law, a form of intellectual property or data ownership, non-certified securities, and other special private law rights.

---

55 Section 6, Payment Services Act, *supra* note 12.

56 Scorechain. (2020, June 18). *Cryptocurrencies regulatory landscape in Singapore.* https://www.scorechain.com/blog/cryptocurrencies-regulatory-landscape-in-singapore/

57 Comply Advantage. (2020, February 28). *Payment Services Act in Singapore*. https://complyadvantage.com/knowledgebase/payment-services-act-singapore/

However, it can be said that one of the most important issues is how to transfer specific rights related to tokens. In either case, the answer varies depending on the economic function and rights of a particular token.

For example, in other jurisdictions, like the UK, as discussed above, although the language varies, a distinction exists between three token categories as follows:

- Payment tokens: These are synonymous with cryptocurrencies and are intended as a means of payment for goods or services, or as a means of value transfer, and do not give rise to claims against their issuer.
- Utility tokens: These provide access to an application or service by means of a blockchain-based infrastructure.
- Asset tokens: These represent assets, such as a debt or equity claim against their issuer. Asset tokens contain a promise, such as a share in future earnings of a company or a project. In terms of their economic function, they are analogous to equities, bonds, or derivatives. Tokens that enable the trading of physical assets on the blockchain (tokenized assets) also fall into this category.

Since these categories are not mutually exclusive, there can also be hybrid tokens. For example, assets and utility tokens can also constitute payment tokens, depending on additional rights. Payment tokens usually do not come with third-party rights. For example, Bitcoin is a pure digital asset. Therefore, according to Swiss law, they can be transferred without written procedures. Although the rules of property law will determine the type of action required to recover illegally disposed assets from the previous owner, in many cases, due to the transnational context of most cases and the universality and purpose of blockchain, this will essentially turn out to be a theoretical transaction.

Different private law rules may apply to public service tokens, which are essentially service vouchers and asset tokens that usually represent promissory notes to third parties. These tokens usually do not represent digital assets but identify the owners of rights against natural or legal persons. This gives rise to the issue of transferability and the question of whether they constitute non-certified securities that can only be transferred in writing. Although it is theoretically possible to use digital signatures to transfer rights under Swiss law, it is currently not possible to do so. The Swiss Federal Council has discussed this issue in a recent consultation on amendments to the Debt Act. According to their proposal, the transfer of rights registered in the registry based on distributed ledger technology will no longer need to be done in writing. If such a change is enacted, it will increase the legal certainty of token transfers. However, it is unclear when or if this amendment will be advanced.

There are currently no DLT-specific laws in force in Switzerland, and comprehensive regulation of tokens or DLT is not contemplated. Rather, the traditional, principle-oriented and technology-neutral approach of Swiss financial market regulation applies. There is a generally published guidance on the regulatory treatment of tokens under Swiss law from the Swiss Financial Market Supervisory Authority (FINMA) — ICO Guidelines. Specifically, FINMA reviews the economic nature of a token to determine its regulatory treatment. For example, whether to treat it as a security. For this, it employs the 'duck test': if it looks like a duck, swims like a duck, and quacks like a duck, then it probably is a duck.

FINMA follows the categorization of crypto assets as payment tokens, utility tokens and asset tokens (as well as hybrid tokens). The regulatory consequences are highly dependent on specific 'token economics' and the rights attached to tokens. However, some general statements are possible to make as follows:

- Payment tokens are not subject to prudential regulations if they are pure digital assets. They may, however, be within the scope of prudential regulation if they convey rights to underlying assets (such as units of gold or any other asset or basket of assets that is relatively 'stable') to token holders, for instance, in the case of certain stable coins. Issuers and traders of payment tokens must comply with Swiss anti-money-laundering laws.
- Utility tokens are not generally within the scope of financial market laws. However, if a utility token also has an investment purpose at the point of issue, FINMA will treat such tokens as securities.
- Asset tokens may qualify as securities, with consequences for both the primary market (i.e., the obligation to publish a prospectus) and the secondary market (e.g., to trade only on licensed securities trading venues, make follow-up disclosures, etc.). They may also fall within the Banking Act, the Collective Investment Schemes Act, and other relevant laws. Therefore, particular attention must be paid when there is an investment component related to an asset, or if the tokens are in some way linked to an underlying asset.

Switzerland is one of the most crypto-friendly jurisdictions. Swiss law does not consider cryptocurrencies legal tender or, consequently, 'money', and does not define the term 'cryptocurrency' or 'virtual currency'. For individuals, cryptocurrencies are seen as assets and are subject to wealth tax, while capital gains on these assets are exempt from income tax. In 2017, the canton of Zug (also known as the Crypto Valley) began accepting Bitcoin and Ether as payment for operating expenses, and Chiasso, in the canton of Ticino, began accepting Bitcoin for tax payments in 2018, with Zug set to follow in 2021.

Therefore, the country's tax collection authority, the Swiss Federal Tax Administration (SFTA) regards Bitcoin and Ethereum as 'assets', which are therefore covered by Switzerland's Wealth Tax and must be declared on yearly returns. The source of funds from cryptocurrency wealth will also need to be listed on tax returns.

Hongkong

There is currently little guidance or judicial consideration as to whether crypto assets will be recognized as 'property' in the law of Hong Kong. The current state of affairs on the treatment of crypto assets as property, the ownership of crypto assets, and their transfer between private individuals is not subject to any legal restrictions or regulations, on condition that they are obtained and/or transferred in good faith. According to their characteristics, crypto assets are sometimes called virtual commodities, cryptocurrencies, digital tokens, or utility tokens, but these are not clearly defined in the law.

The term 'virtual assets' was adopted by Hong Kong's Securities and Futures Commission (SFC) to represent this broad class of instruments, stating that "the polymorphous and evolving features of virtual assets mean that they may be, or claim to be, a means of payment, may confer a right to present or future earnings or enable a token holder to access a product or service, or a combination of any of these functions."

Even so, in the regulatory treatment of crypto assets, Hong Kong regulators have made it clear that crypto assets could be subject to regulation under existing regulatory regimes, and this may include, currency, securities, or futures contracts, depending on the features and characteristics of each crypto asset. For example, the Chief Executive of the Hong Kong Monetary Authority (HKMA) considered the extent to which cryptocurrencies could serve as money, by measuring them against the following three benchmarks, which are: (i) a medium of exchange (i.e., whether it is generally

accepted as a means or instrument of payment to facilitate the sale and purchase of goods and services); (ii) a store of value (i.e., the ability to hold its value over time); and (iii) a unit of account (i.e., whether it is accepted as a standard measure of value or price of goods, services, assets, liabilities, income, expenses, profits, and losses). From the HKMA's perspective, cryptocurrency does not satisfy the criteria of 'money' primarily because of its failure to be readily accepted as a medium of exchange, its high volatility in value arising from its lack of intrinsic worth, and the difficulty in adopting cryptocurrency as a standard measure of value.

Further to that, there are various statement issued by the SFC suggesting that crypto assets could, depending on their characteristic, fall within the meaning of 'securities', which includes interests in a collective investment scheme, or 'futures contracts'. In order to allow crypto asset-related activities to fall within the safety net provided by the existing regulatory framework, the SFC implemented a number of regulatory policies in November of 2018 to address the management and distribution of crypto asset funds or portfolios by intermediaries that hold licenses to be intermediaries from the SFC. The SFC has also launched a regulatory sandbox to explore the feasibility of regulating and licensing crypto asset trading platforms.

As many ICO issuers have established business bases in Hong Kong and opened their activities to Hong Kong residents, the SFC (i.e., the local securities regulatory authority) issued a statement on ICOs on September 5, 2017, warning the public about the risk of participating in ICO campaigns. It also warms the public that ICO tokens that possess features of 'securities' as defined under the Securities and Futures Ordinance (Cap. 571) (SFO) would need to be authorised by the SFC unless an exemption applies, and that dealing in and advising on securities-based ICOs would be a regulated activity under the SFO. Hence, such activity should only be carried out by corporations that are licensed.

The HKMA and the SFC have recognized Bitcoin and other similar currencies as 'virtual commodities.' However, it unclear if and how this extends to other altcoins, which are a sub-category of 'virtual assets', and Hong Kong has not established new legislation or regulations to define those terms. That said, while there has been no further clarification from the SFC on which tokens or coins may fall under the new asset class of 'virtual assets, it has acknowledged that many virtual assets do not necessarily amount to 'securities' or 'futures contracts' for the purpose of the SFO, and it has particularly confirmed Bitcoin and Ether as examples that may be referred to as 'Non-SF Virtual Assets'.

How is public policy being interpreted?

Indonesia

In the ASEAN+6 context, we can see, for example, Indonesia's adoption of a wider position in the case of *Bankers Trust v PT Mayora Indah Tbk* (2000)[58] and *Astro Nusantara Bvetal v PT Ayunda Primamitra* (2010),[59] where the definition of Public Policy was interpreted too widely by the Indonesian court. Furthermore, Presidential Regulation No. 34 of 1981 contains only two paragraph and does not mention which court has the authority to deal with requests for enforcement of foreign arbitral

[58] The Decision of the Supreme Court No. 02 K/Ex'r/Arb.Int/Pdt/2000. Some authors have discussed this case, among others, Karen Mills, Enforcement of Arbitral Awards in Indonesia & Other Issues of Judicial Involvement in Arbitration, Paper, February, 2003, revised February, 2005; Mutiara Hikmah, Loc.cit.

[59] The Supreme Court Decision No. 01 K/Pdt.Sus/2010. Some authors have discussed this case, among others, Mills, 2006; Kristy & Jing, 2013.

awards in Indonesia. It is also silent on the application of public policy, as incorporated in article V of the New York Convention.

Another interesting case to look at would be *PT Nizwar v Navigation Maritime Bulgare*, where the Indonesian Supreme Court refused to execute a request for the enforcement of a London arbitration award. The Supreme Court argued that the court could not enforce the award, mainly because there was no implementing legislation (of the Government Regulation No. 34 of 1991) that gave the Court of Jakarta the power to enforce the foreign arbitration award (in Indonesia).

On this development, in August of 1999, the Indonesian Supreme Court put into effect Law No. 30 of 1999 on Arbitration and Alternative Dispute Resolution. This replaced the old Dutch-private procedural law on arbitration, as provided in article 615–651.[60] Law No. 30 of 1999 regulates both domestic and international arbitration and their awards. It is worth noting that Article 66 provides for the requirement of public policy and states that international arbitration awards will only be recognised and enforced within the jurisdiction of the Republic of Indonesia if they fulfil the following requirements:

(a) the international arbitration award must have been rendered by an arbitrator or arbitration tribunal in a country which, together with the Republic of Indonesia, is a party to a bilateral or multilateral treaty on the recognition and enforcement of international arbitration awards;

(b) international arbitration awards, as contemplated in item (i), are limited to awards which, under the provisions of Indonesian law, fall within the scope of commercial law;

(c) international arbitration awards, as contemplated in item (i), may only be enforced in Indonesia if they do not violate public order;

(d) international arbitration awards may only be executed in Indonesia after obtaining execution from the head of the Central District Court of Jakarta; and

(e) when one of the parties involved in the international arbitration is the State of the Republic of Indonesia, the international arbitration may only be enforced if it has obtained execution from the Supreme Court, in which the power will be delivered to the head of the Central District Court of Jakarta.

However, it worth noting that the explanatory notes of Article 66 of Law No. 30 of 1999 still do not provide a clear explanation on what the term 'public policy' means. Hence, this lack of definition would imply that the broad definition expressed under Supreme Court Regulation No. 1 of 1990 still applies. This would mean that the term 'public policy' could still be extensively interpreted.

Notwithstanding the above, the good news is that Indonesia has taken a mixed approach towards cryptocurrencies such as Bitcoin, Ethereum, Dash, Litecoin, and Ripple. Indonesia's Commodity Futures Trading Regulatory Agency (known as Bappedti) has approved regulation No. 5/2019 (February 2019), which does recognise Bitcoin and other cryptocurrencies as trading commodities, giving legal certainty to the cryptocurrency exchanges already operating in the country. It should be noted that the law imposes AML/CFT requirements on virtual asset service providers, and cryptocurrencies are banned as domestic payment instruments under the Bank Indonesia Regulation No. 18/40/PBI.2016 on the Implementation of Payment Transaction Processing (November 2016).

[60] Articles 615 to 651 Rv did not contain the provisions on public policy as the grounds for the annulment of (foreign) arbitration awards. This suggested that Rv on arbitration seemed to regulate the domestic arbitration. The Rv on arbitration was divided into five parts. Part 1 regulated the appointment of arbitrators (articles 615–623); part 2 was the provisions on arbitration proceedings (articles 624–630); part 3 regulated the arbitration awards (articles 631–640); part 4 was on the efforts or measures against the arbitration award (Articles 641–647); and part 5 contained the provisions concerning the end of arbitrators' duty (articles 648–651).

This would mean that, by having cryptocurrencies recognized as trading commodities, it is likely that potential smart contract disputes can be resolve by arbitration, as they are approved and recognized as trading commodities in Indonesia, and it can be said that they have already cleared the public policy hurdle.

Malaysia

Malaysia's earlier position on the enforcement of international arbitral awards can be found in the case of *Jan De Nul (Malaysia) Sdn Bhd Anor v Vincent Tan Chee Yioun Anor*[2018] 1 LNS 1615,[61] where both parties challenged the Award, applying to refer to questions of law arising out of the Award pursuant to section 42 of the Arbitration Act (the 2005 Act).[62] Both parties also raised the preliminary objections that section 42 of the 2005 Act is inapplicable in this case, as the arbitration between them was an "international arbitration" within the meaning of section 2 of the 2005 Act.[63] Further, section 3(3) of the 2005 Act[64] provides that section 42 of the Act (which is contained within part III of the 2005 Act) has no application unless the parties had agreed in writing for it to be applicable.

Essentially, section 42 allows for the court's intervention by allowing the parties to refer to the court on questions of law arising out of an arbitral award. The court will then have power to confirm, vary, set aside, or to remit the award to the tribunal for reconsideration. This can also cause problems in terms of uncertainty in enforceability. However, in the case of *AJWA For Food Industries Co (MIGOP), Egypt v. Pacific Inter-Link Sdn Bhd & Anor (*AJWA case)[65], the Court of Appeal has held that section 42 of the 2005 Act may be relied on if the arbitration agreement is governed by Malaysian law as the governing law.

However, the Federal Court had reversed the AJWA decision and held that, although the agreement had used Malaysian law as the governing law of the contract, this cannot be interpreted and equated to an agreement to include part III and section 42 of the 2005 Act. So now, it can be seen that this decision had clarified this point of law and ensured certainty. Furthermore, section 42 of the 2005 Act has been repealed by the Amendment Act 2018.[66]

Given this development, in dismissing JDN and Sofidra's appeal to set the award aside for breach of the public policy of Malaysia, because there was a breach of the rule of natural justice about the making of the award, the Federal Court upheld the decision of both the High Court and the Court of Appeal; it also affirmed the distinction between the application of section 37 and section 42 which can be found in the case of *Petronas Penapisan (Melaka) Sdn Bhd. v. Ahmani Sdn Bhdn* ("Petronas Penapisan"),[67] where the Court of Appeal held that section 37 application relates to the award making process, while section 42 application relates to the award itself (i.e. whether the award contains an error that substantially affects the rights of one or more of the parties). Now, with section 42 of the 2005 Act repealed, we can be certain that there are limited circumstances where parties can seek intervention from the courts.

It should also be noted that Malaysia's Federal Court approved the following passage of the Singapore Court of Appeal in *PT Asuransi Jasa Indonesia (Persero) v Dexia Bank*:

---

61 *Jan De Nul (Malaysia) Sdn Bhd Anor v Vincent Tan Chee Yioun Anor* [2018] 1 LNS 1615.

62 Arbitration Act 2005, s42.

63 Arbitration Act 2005, s2.

64 Arbitration Act 2005, 3(3).

65 *AJWA For Food Industries Co (MIGOP), Egypt v. Pacific Inter-Link Sdn Bhd & Anor* (AJWA case).

66 Arbitration (Amendment) (No 2) Act 2018.

67 *Petronas Penapisan (Melaka) Sdn Bhd. v. Ahmani Sdn Bhd* [2016] 3 CLJ 403 ("Petronas Penapisan").

"...the general consensus of judicial and expert opinion is that public policy under the Act encompasses a narrow scope. In our view, it should only operate in instances where the upholding of an arbitral award would 'shock the conscience'... or is 'clearly injurious to the public good or... wholly offensive to the ordinary reasonable and fully informed member of the public'... or where it violates the forum's most basic notion of morality and justice."[68]

The apex court went on to say:

"***[55]****...However, it must be appreciated that the concept of public policy generally is itself a broad concept. But in applying the concept for the purpose of setting aside an award... the concept of public policy ought to be read narrowly and more restrictively. The court's intervention should be sparingly used. The court must be compelled that a strong case has been made out that the arbitral award conflicts with the public policy of Malaysia... "The concept of public policy must be one taken in the higher sense where some fundamental principle of law or justice is engaged, some element of illegality, where enforcement of the award involves clear injury to public good or the integrity of the court's process or powers will be abused."*[69]

Singapore

When it comes to the setting aside of international arbitral awards on grounds of offending public policy, we can see Singapore's position on this matter in the case of *PT Asuransi Jasa Indonesia (Persero) v Dexia Bank*. We can also see that the apex court of Malaysia also approved Singapore's position in this case, as mentioned above. Another interesting case to note is *Sui Southern Gas Co Ltd v Habibullah Coastal Power (Pte) Ltd* [2010] SGHC 62[70], where the High Court had to decide whether to set aside an arbitral award on the grounds that the decision was "perverse and irrational". However, the Court in choosing not to set aside the award demonstrated that it is prepared to show deference towards the decision of the arbitral tribunal. Further, Judith Prakash J also held that arbitral tribunal awards will only be set aside where the grounds for setting aside set out in the International Arbitration Act ("the IAA") are strictly complied with.

It should be noted that it was alleged that the award in dispute should be set aside as it was perverse and irrational. This was relied on as an independent ground for setting aside, and to further support the application to set the award aside, Article 34, Schedule 1 of the IAA[71] was also relied upon, that the award went beyond the scope of the submission to arbitration, and that it was in conflict with public policy. The Court rejected the application on all three grounds. The Court also rejected the argument at the threshold stage and held that the contention of breach of public policy cannot be vague and generalized (*John Holland Pty Ltd v Toyo Engineering Corp* (Japan) [2001] 1 SLR (R) 443.[72] And since SSGC failed to identify any particular public policy of Singapore that was breached, the argument had failed.

In spite of that, the Court did go on to consider SSGC's dispute that public policy would operate whenever upholding the award would "shock the conscience", which was alleged to be the case. However, the three aspects that were mentioned by the Court are worth noting, and they are, (i) the court did not accept that the "shock the conscience" test could stand alone as the test for whether public policy would operate, (ii) a very high threshold must be crossed, and shocking circumstances

68 *PT Asuransi Jasa Indonesia (Persero) v Dexia Bank* [2006] SGCA 41.

69 *PT Asuransi Jasa Indonesia (Persero) v Dexia Bank* [2006] SGCA 21.

70 *Sui Southern Gas Co Ltd v Habibullah Coastal Power (Pte) Ltd* [2010] SGHC 62.

71 Article 34, Schedule 1, International Arbitration Act.

72 *John Holland Pty Ltd v Toyo Engineering Corp* (Japan) [2001] 1 SLR (R) 443.

such as corruption, bribery or fraud, which would contravene the most basic notions of morality and justice, must be shown, and (iii) an assertion that the Award was "perverse and irrational" cannot, in itself, amount to a breach of public policy.[73]

India

Whilst Singapore's and Malaysia's position is promising, as to giving greater certainty to the enforcement of international awards, India's position is also of interest. While some countries consider public policy to mean international public policy, India is one of the few countries to statutorily define public policy through its Arbitration and Conciliation (Amendment) Act 2015.[74]

In the case of *Renusagar Power Co. Ltd v. General Electric Co 1994* Supp (1) SCC 644, the Indian courts have held that there is no workable definition of international public policy, therefore, it should be construed to be the doctrine of public policy applied by the courts in India.[75] India has also statutorily included the grounds of fraud, corruption, fundamental policy of Indian law, and basic notions of justice and morality within the definition of public policy. While it is mentioned that public policy has no definition, its elements have been identified statutorily in section 48(2)(b)(ii) of the Arbitration and Conciliation (Amendment) Act 2015.[76]

In *Renusagar Power Co. Ltd v. General Electric Co*, it should be noted that the Supreme Court stressed the fact that interference on the merits of the arbitral award would be outside the consciousness of Section 48 of the *Arbitration & Conciliation Act 1996*. Interestingly, *Renusagar* had provided a narrow scope of the grounds under section 48.

Indian Courts had over the years increasingly limited their interference with arbitral awards. This approach of non-interference is more prevalent, especially when it comes to the enforcement of foreign awards under Section 48 of the Arbitration and Conciliation Act 1996.[77] As we can see, this approach was reaffirmed in the recent case of *Vijay Karia and Ors. v. Prysmian Cavi E Sistemi SRL & Ors,*[78] where the Supreme Court dismissed the appeal and came down heavily on the Appellants for engaging in conjectural litigation and attempting to invoke the limited power of the Supreme Court to resist foreign award enforcement only under Article 136 of the Constitution of India.[79] The Supreme Court also gave further importance to the wider meaning given to 'public policy of India' in the case of *Shri Lal Mahal Ltd. v Progetto Grano SpA*, where it opined that, in the domestic sphere, the wider meaning of 'public policy of India' would not apply to section 48(2)(b) of Section 48 of the Arbitration & Conciliation Act 1996.

Finally, it is opined that Section 48 of the *Arbitration & Conciliation Act 1996* gives effect to *Article V of the New York Convention,* in which it set forth the limited and exhaustive grounds on which recognition and enforcement of an arbitral award may be refused by a competent authority in the Contracting State where recognition and enforcement is sought. The Indian judiciary had repeatedly emphasized over the years that the grounds for resisting enforcement of foreign awards under section 48 of the said Act are extremely limited and cannot be read in the same manner as the grounds available for challenging an award under section 34 of the said Act.[80]

---

73 *John Holland Pty Ltd v Toyo Engineering Corp* (Japan) [2001] 1 SLR (R) 23.

74 Arbitration and Conciliation (Amendment) Act 2015.

75 *Renusagar Power Co. Ltd v. General Electric Co 1994* Supp (1) SCC 644.

76 Arbitration and Conciliation (Amendment) Act 2015, 48(2)(b)(ii).

77 Arbitration and Conciliation Act 1996, s48.

78 *Vijay Karia and Ors. v. Prysmian Cavi E Sistemi SRL & Ors.*

79 *Constitution of India, Article 136.*

80 *Arbitration & Conciliation Act 1996, s34.*

China

While the positions of the abovementioned countries are certain in recognising and enforcing foreign arbitral awards, the Chinese Courts have a different position when it comes to the enforcement of foreign arbitral awards in the name of public policy. In *Civil Ruling Yue 03 Min Te No 719 (26 April 2020)*, the Shenzhen Intermediate People's Court set aside an award made by a local arbitral institution in Shenzhen on virtual currency where it deals with public policy as an infringement on China's public interest and policy (i.e., that the order and stability of financial markets as part of Chinese mainland society was under threat). The Supreme People's Court of China (SPC) later approved the decision of the Shenzhen court in setting the award aside.[81]

The arbitral tribunal found that the asset manager was in breach of contract and awarded the US dollar equivalent of the value of the cryptocurrencies plus interest. The asset manager then applied to the court to set aside the award, and that application succeeded. The award was set aside for the following reasons, (a) the arbitral award is in breach of public policy, (b) A 'Notice on Precautions Against the Risks of Bitcoins' had been issued by five PR China authorities, including the People's Bank of China, stating that Bitcoins do not have the legal status of a currency and shall not therefore be circulated or used in the market, (c) An 'Announcement on Preventing the Financing Risks of Initial Coin Offerings' had been issued by seven PR China authorities, including the People's Bank of China, according to which token fundraising and exchange platforms shall not (i) provide exchange services between tokens and fiat currency and between cryptocurrencies; (ii) buy or sell tokens for cryptocurrencies, or act as central counterparts facilitating the trading of tokens for cryptocurrencies; or (iii) provide pricing or information intermediary services for the exchange of tokens for cryptocurrency, (d) the effect of the Notice and the Announcement respectively was to prohibit illegal activities that would otherwise cause disruption to financial order and stability, and (e) the award, if allowed to stand, would have had the effect of facilitating circulation of Bitcoins in PR China and would therefore disrupt the integrity and security of the financial system of PR China and, as a result, its public policy.

On the other hand, the Master plan on ASEAN Connectivity 2025 estimates that digital technologies in ASEAN could potentially be worth up to US$625 billion — 8 per cent of ASEAN's GDP by 2030 — which may be derived from increased efficiency, new products and services, etc., where smart contracts can be a driving force.[82] Therefore, it is important to not just have recognition of the enforceability of smart contracts by the local courts, as in the Singapore case of *B2C2 Ltd v Quoine Pte Ltd.*[83] It is also vital for Governments to play an active role in shaping policy for smart contracts moving forward.

Although there is a Masterplan with the objective to further ASEAN's Connectivity by 2025, given the growing demand to use contracts, digital transformation could still be a challenge for almost every aspect of the economy and society. This implies that many different policy areas need to be considered in a whole-government response. Therefore, it requires governments to reach across traditional policy and across different levels of government to develop a whole-of-government approach to policymaking.

Apart from the policy front, is it imperative to look at the way in which the law in various jurisdictions, either now or in the future, will be subject to the principle of the law of contract. This means that there would be a need to establish a proper legal framework for smart contracts. Contracts can

[81] *Civil Ruling Yue 03 Min Te No 719 (26 April 2020).*

[82] Wong, S., & Low, D. (2019, February 15). *Forging ahead on Southeast Asia's digital journey*. The Business Times. https://www.businesstimes.com.sg/asean-business/contributions/forging-ahead-on-southeast-asia%E2%80%99s-digital-journey

[83] *B2C2 Ltd v Quoine Pte Ltd* [2019] 4 SLR 17.

be considered an agreement involving two or more parties to comply with a series of conditions. Whatever the form, they must include fundamental elements such as voluntary consent of the parties, the object of the contract, and a fair cause that is true and lawful. They only differ in ways of writing, their legal implications and ways of compliance (Cons & Hernández, 2019).

In the ASEAN+6 region, Singapore, Malaysia and India would be most likely to recognize and enforce foreign arbitral awards, compared to Indonesia and China, as discussed above. Hence, we are of the opinion that, given the uncertainties revolving around smart contracts, arbitration would be the preferred medium in resolving smart contract disputes.

Is there a discernible trend in applying public policy considerations to smart contract/ virtual asset disputes?

Having explored in particular the aspects of (a) the public policy consideration with regards to the recognition of smart contracts, and (b) the regulatory treatment of cryptocurrencies by various jurisdictions, it is fair to say that the general position of arbitration-friendly countries is to uphold foreign arbitral awards in smart contract disputes, and that a smart contract is capable of fulfilling contractual principles.

However, a particular jurisdiction to note would be China, in its position regarding the treatment of foreign arbitral awards relating to smart contracts and the recognition of cryptocurrencies, in which it had adopted a narrow approach in its interpretation of public policy, that can be found in the "Shenzhen case", as discussed above. The Supreme People's Court of China (SPC) later approved the decision of the Shenzhen court in setting the award aside[84] in the view that, by upholding the foreign arbitral award in that case, it would contravene public policy and disrupt the order and stability of the financial market.[85]

In contrast to China, Japan for example arguably has the world's most progressive regulatory climate for cryptocurrencies. Cryptocurrency exchange businesses operating in Japan have been regulated by the Payment Services Act ("PSA") since June 3, 2016.[86] Furthermore, we can see from our extensive discussion in Chapter 3 regarding the topic of whether 'cryptocurrencies are property?', that some emerging economies have, be it directly or indirectly, recognized cryptocurrencies as property.

After the recent crackdown against cryptocurrencies this year with action taken against miners and curbs imposed on crypto banking services and trading in China, there was a significant shift in tone mid-July 2021, with China's central bank now calling Bitcoin an 'investment alternative'. It is suggested that China realized its recent crackdown would have an adverse effect, hindering its plan to become a powerful centre of finance and an economic powerhouse, amongst other reasons that may or may not be known.

We can see this significant shift in Beijing's tone on cryptocurrencies issuance and trading. Li Bo, deputy governor of the PBOC, said during a panel hosted by CNBC at the Boao Forum for Asia that, "We regard Bitcoin and stable coin as crypto assets... These are investment alternatives". He also added that, "They are not currency per se. And so the main role we see for crypto assets going forward, the main role is investment alternative."

As investment alternatives, "many countries, including China, are still looking into it and thinking about what kind of regulatory requirements. Maybe minimal, but we need to have some kind of regulatory requirement to prevent... the speculation of such assets to create any serious financial

[84] *Civil Ruling Yue 03 Min Te No 719 (26 April 2020).*

[85] *Civil Ruling Yue 03 Min Te No 719 (26 April 2020).*

[86] Payment Services Act, Act No. 59 of 2009, amended by Act No. 62 of 2016.

stability risks," Li said.[87] He added that the central bank will keep its current regulations on cryptocurrencies.

Although there already was a discernible trend toward applying public policy considerations to smart contract and virtual asset disputes in the various jurisdictions, as discussed above, it can be said, based on the significant shift in Beijing's tone on cryptocurrency issuance and trading, that, in the future, there will be a discernible trend towards applying public policy considerations to smart contract and virtual asset disputes in favour of recognizing smart contracts and virtual assets, particularly in China. Until then, this significant development toward the enforcement of foreign awards in relation to smart contracts and virtual assets in China is good news for investors.

In the case of *Civil Ruling Yue 03 Min Te No 719 (26 April 2020)*, the arbitral tribunal found that the asset manager was in breach of contract and awarded the US dollar equivalent of the value of the cryptocurrencies plus interest. However, would there be a problem making the award in cryptocurrency as opposed to the equivalent in regular currency (e.g. USD or SGD)?

Cryptocurrencies can be used to pay for goods and services, as well as for investing in some areas around the world. In this respect, they are similar to physical currencies. However, unlike fiat money, cryptocurrencies have no physical form, nor have they been declared legal tender in most countries, except for El Salvador, which became the first country to adopt Bitcoin as legal tender, enacting legislation that will take effect in September 2021.

However, making arbitral awards in cryptocurrencies would give rise to uncertainty in terms of the exact value to be awarded in smart contract disputes. For example, Bitcoin is much more volatile than the dollar. From June 8 to June 15 2021, its value swung between US$32,462 and US$40,993, and in the period from May 15 to Jun 15 2021, it ranged from US$34,259 to US$49,304.[88]

In the case of *Civil Ruling Yue 03 Min Te No 719 (26 April 2020)* ("Shenzhen case"), the company and Li sought arbitration to establish that (a) the Shares be transferred to Gao, (b) CNY 250,000 be paid by Gao to the Company, (c) USD 493,158.40 (equivalent of 20.13 BTC, 50 BCH and 12.66 BCD) and interest be paid by Gao to Li, and(d) an additional CNY 100,000 be paid by Gao to Li for breach of the Contract. It is reasonable to believe that the tribunal at that time would be faced with tremendous uncertainty, due to the volatility of Bitcoin.

In the Shenzhen case, the arbitral tribunal ingeniously determined USD 401,780 to be the equivalent of 20.13 BTC, 50 BCH, and 12.66 BCD, plus interest to Li, by "taking reference" of the closing price at the material day from the website okcoin.com. Therefore, by way of example as seen in the Shenzhen case, it is suggested that arbitral tribunals are able to determine the value to be awarded in smart contract disputes involving cryptocurrencies by taking reference of the closing price at the material day from a reliable source like okcoin.com. New financial public policy is going to get more pronounced in China.

For the sake of clarity, a blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without the need for a central clearing authority. Potential applications can include fund transfers, settling trades, voting, and many other issues. Unlike a central bank where all the transactions are verified, processed and

[87] Haldane, M. (2021, July 16). *China's bitcoin crackdown: Why is it happening and what's next for the original cryptocurrency?* South China Morning Post. https://www.scmp.com/tech/big-tech/article/3141253/chinas-bitcoin-crackdown-why-it-happening-and-whats-next-original

[88] Subacchi, P. (2021, 25 June). Commentary: Bitcoin is now legal tender in one country. Regrets may soon follow. *CNA*. https://www.channelnewsasia.com/commentary/commentary-el-savador-just-made-bitcoin-legal-tender-it-s-a-big-1938056

recorded in a centralized private ledger, in Bitcoin, every user acts as a bank and keeps a copy of this ledger. In Bitcoin, the role of the distributed ledger is played by the so-called *blockchain*. There are of course benefits and challenges in using centralized or decentralized ledgers; however, it is not the main purpose of this paper to discuss these technical issues.

At this juncture, it is possible to suggest where the trend is moving in terms of public policy. Some countries are less concerned about traditional public policy regarding smart contracts and/or virtual assets. Various countries in the ASEAN+6 region are beginning to accept that public policy has to be interpreted narrowly when using it as a ground for setting aside foreign arbitral awards.

And even in the ASEAN+6 region where there is little to no case law to determine the recognition of smart contracts and virtual asset disputes, it is evident that steps have been taken by domestic authorities (such as Indonesia, Singapore, the United States, the United Kingdom, Australia, Switzerland, Hong Kong and Malaysia) in their acceptance, or to adopt a mixed approach to cryptocurrencies by enacting new national laws and regulations. One such jurisdiction is Indonesia. This is a promising sign that the recognition of smart contracts and cryptocurrencies is a work in progress and its approach favors a narrow interpretation of public policy in the setting aside of foreign arbitral awards. For the avoidance of doubt, jurisdictions such as Malaysia, Singapore and India have adopted a narrow approach to public policy interpretation when it comes to setting aside foreign arbitral awards.

Are there jurisdictional issues and challenges in terms of public policy?

In Chapter 4 on public policy considerations in smart contract disputes, it is shown that some jurisdictions such as Indonesia and China would adopt a wider position in terms of public policy considerations when it comes to smart contract disputes. In the process of drafting the arbitration agreement, parties would need to consider carefully, (a) the seat of arbitration and the applicable laws that would govern the dispute, as well as (b) how national courts will apply public policy considerations when being asked to set aside an award (at the seat) or to refuse to grant recognition and enforcement.

Considering hypothetically, if the parties have chosen China to seat the arbitration and Chinese law to be the applicable law that will govern the dispute, it is clear that either party will be faced with the possibility of the award being set aside in the event it is challenged in the name of public policy, a clear example of which would be the Shenzhen case, where the Supreme People's Court of China (SPC) later approved the decision of the Shenzhen court in setting the award aside.[89]

That brings us to the next question regarding arbitrability. Is a smart contract involving cryptocurrencies arbitrable? It may well be said that smart contract disputes involving cryptocurrencies are not arbitrable, as this is deemed to contravene some jurisdiction's public policy (e.g., China and Indonesia, which adopt a wide position in their interpretation of public policy).

So what is arbitrability? It relates to whether a type of dispute can or cannot be settled by arbitration. It also answers the question of whether a subject matter of claim is or is not reserved to the domain of domestic courts, under the provision of national laws. For example, if the dispute is not arbitrable, the arbitral tribunal is limited in its jurisdiction and the claim must be submitted to domestic courts instead.

Certain disputes may involve sensitive public policy issues (i.e., smart contracts that involve cryptocurrencies) that have to be left exclusively to the jurisdiction of domestic courts by their own laws, as it is seen in the Shenzhen case. The arbitrability of a dispute is territorial due to the different

[89] *Civil Ruling Yue 03 Min Te No 719 (26 April 2020).*

policy considerations, and it also depends on how open a State is to arbitration. Non-arbitrability of a dispute will render the arbitration agreement invalid, resulting in the lack of jurisdiction of the tribunal, and the award might not be recognized and enforced.

The concept of arbitrability can be found in Article 2, paragraph 1, of the New York Convention, which provides that each contracting State shall recognize an agreement in writing "*concerning a subject-matter capable of settlement by arbitration*".[90] In addition to arbitrability, Article 5, paragraph (2)(a) also states that recognition and enforcement of an arbitral award may be refused if the court where such recognition and enforcement is sought finds that "*subject matter of the difference is not capable of settlement by arbitration under the law of that country*".[91]

Pursuant to Article 1, paragraph 5 and Article 34, paragraph 2(b) of the UNCITRAL Model Law on International Commercial Arbitration also address the issue of arbitrability;[92] however, the former did not specify which matters are arbitrable, and the latter only stipulates that the arbitral award may be set aside provided, among others, the court finds that the subject matter of the dispute is not capable of settlement by arbitration under the law of that State. In Articles II and V of the New York Convention can also be found the law of arbitrability as a ground for a court to refuse to recognize and enforce an award. However, it is silent as to which law should govern the question of arbitrability at the pre-award stage.[93]

On the issue of arbitrability, it is a matter of national public policy and sometimes social policy. For example, in the Shenzhen case, the question of arbitrability could be raised as smart contract and virtual assets disputes (i.e., the subject matter of the dispute) are deemed not capable of settlement by arbitration under the law of that State. Hence the governing law of an arbitration agreement does matter, especially when it involves international contracting parties in a smart contract.

To ensure enforceability, the arbitral tribunal should generally determine arbitrability with reference to specific laws of the place of arbitration. In the event a dispute is not arbitrable according to the relevant laws of the place of arbitration, parties will face a risk of setting aside procedures in that country, and this may also affect its enforcement in another country.

Therefore, to deal with the issue of how national courts will apply (a) public policy considerations when being asked to set aside an award (at the seat) or to refuse to grant recognition and enforcement, and (b) the applicable laws that would govern the dispute, it is suggested that, to get over the issue of applicable law and issues around the subject matter (e.g., cryptocurrencies in some jurisdiction that does not recognize cryptocurrencies as arbitrable and are smart contract arbitrable), parties can either adopt the Supranational framework or the UNIDROIT principle of the law of contract.

It should be noted that "where there is no express choice of law governing the arbitration agreement, there is a strong presumption that the parties have impliedly chosen the law of the seat. That is the case even where the law governing the main contract differs from that of the seat, and the governing law of the arbitration agreement determines its interpretation, scope and validity."[94]

For example, supranational law like the Hague Principles on Choice of Law in International Commercial Contracts 2015 (the "Principles") or the UNIDROIT principles of the law of contract are some options parties can choose that will help in governing the dispute, especially on the issue of arbitrability, as the law of the seat would apply, and this will contribute to the issue of whether or

90 Article 2, paragraph 1, New York Convention.

91 *Article 5, paragraph (2)(a),* New York Convention.

92 Article 34, paragraph 2(b), UNCITRAL Model Law on International Commercial Arbitration.

93 Articles II and V, New York Convention.

94 *Enka Insaat ve Sanayi SA v OOO "Insurance Co Chubb" & ors* [2020] EWCA Civ 574, [2020] EWCA Civ 574.

not cryptocurrencies are property. As far as the governing law of the substantive law is concerned, a supranational framework can help avoid issues around smart contract recognition under the governing law for the contract if the parties are from jurisdictions that are still work-in-progress in recognizing smart contracts and virtual assets.

International smart contracting parties can choose the Hague Principles on Choice of Law in International Commercial Contracts 2015 (the "Principles") as the choice of law. Firstly, it recognises in principle that contracting parties can choose delocalised rules of law to govern their contract, provided they are "generally accepted on an international, supranational or regional level as a neutral and balanced set of rules" (Article 3).[95]

This means that parties can independently select, for example, the Vienna Convention on the International Sales of Goods to govern their contract, without explicitly choosing the law of a country which has enacted the Convention into its law. The Principles will probably disallow a simple choice of lex mercatoria since it would not meet the requisite level of acceptance at least as far as the contents ("set of rules") are concerned. Lastly, the Principles provides that whether a choice of Supranational rules of law is possible is a matter for the law of the forum, and the Principles has deliberately left it to each jurisdiction to decide whether to allow this type of choice in litigation and arbitration contexts respectively. Therefore, it is possible for contracting parties to choose the Principles to regulate the effects of their choice of law agreement in their contract, and this could work in the context of international arbitration.

Alternatively, international smart contracting parties can also choose UNIDROIT principles as the choice of law to govern the substantive contract. The objective of doing so is the same as that of choosing a Supranational law as discussed above. The fundamental reason why the international contracting parties should be advised to opt for the express choice of the UNIDROIT Principles in combination with international arbitration is the higher likelihood that their contract will be recognized and given effect to the maximum extent that is legally and practically obtainable.

If a given national law is expressly selected as the applicable law on the ground that it is favourably disposed towards not recognizing a smart contract as a contract and/or virtual assets as property, parties will then run into overarching issues of the award being challenged on jurisdiction and arbitrability, ultimately leading to issues of enforceability of foreign awards relating to smart contract disputes and/or cryptocurrencies.

The UNIDROIT Principles constitute an authentic novelty among the legal instruments applicable to international commercial contracts.[96] While most international uniform law instruments, be they of a legislative or non-legislative nature, are restricted to particular types of transaction (sales, leasing, carriage of goods by sea, road, or air, and so on) or to specific topics (delivery terms, modes of payment, and so on), the Principles provide a comprehensive set of principles and rules relating to international commercial contracts in general, comparable to the—codified or unwritten— general part of contract law found in domestic law. Indeed, they cover a wide range of subjects such as freedom of contract, good faith and fair dealing and usages, as well as contract formation including contracting on the basis of standard terms, interpretation, validity including illegality, third party rights, conditions, performance, non-performance and remedies, set off, assignment of rights, limitation periods, plurality of obligors and of obliges, and so on (Bonell, 2018).

[95] Hague Principles on Choice of Law in International Commercial Contracts 2015, Article 3.

[96] 'Perhaps the most interesting development of the last quarter of the 20th century'. (Goode, 2005).

In Article 3 of the Hague Principles, the 'rules of law that are generally accepted on an international, supranational or regional level as a neutral and balanced set of rules'[97], and the Official Commentary expressly mentions the UNIDROIT Principles as an example of such rules of law capable of being chosen as the governing law.[98] And according to the Hague Principles, parties may choose such non- State 'rules of law' as the law governing their contract only if the law of the forum does not provide otherwise.[99]

It has been seen previously that due to public policy considerations, it is possible that countries will not accept (a) smart contracts as contracts, (b) cryptocurrencies as property, and/or (c) enforcing foreign awards that relate to smart contract disputes and/or cryptocurrencies. Therefore, having the smart contract governed by the UNIDROIT principles of the law of contract is another possible way out of the deadlock. That will mean that it would be for the parties to submit their dispute to arbitration and to choose, as they nowadays may, according to most national arbitration laws, non-State 'rules of law' (i.e. UNIDROIT principles) as the law applicable to the substance of their disputes.[100] However, if the parties do not opt for such a solution, the determination of the applicable law will be left to the relevant conflict-of-laws rules, with all of the uncertainties, such as, (a) resorting to a 'neutral' law—that is, the law of a third country—that is foreign to both of them, and to know its content may require time-consuming and expensive consultations with lawyers of that country, and (b) due to the different national rules of private international law, parties risk remaining uncertain as to the law governing their contract until the competent forum is established. Even then, depending on the conflict-of-laws rules of the forum, the same contract may well be subject to the law of State X or to the law of State Y (Baptista, 1995).

Therefore, it may be suggested that Supranational laws can help parties avoid the uncertainties of not having their smart contracts recognized and/or having the foreign arbitral award set aside relating to smart contracts and cryptocurrencies.

Finally, there is going to be an increase in the number of smart contracts and cryptocurrencies being used widely. Hence, as time goes by, smart contracts are probably going to be used in other contexts and in other contractual situations, not only cryptocurrencies. Therefore, it is imperative for lawyers to grasp the direction of the trend, in terms of public policy concerning smart contracts and cryptocurrencies.

---

97 The more concise formulation of Art. 5 of the Paraguayan Law reads 'rules of law of a non-State origin that are generally accepted as a neutral and balanced set of rules'.

98 Cf. Comment 3.6 ('[R]ules of law' that would satisfy this . . . criterion may [be] non-binding instruments formulated by established international bodies. One example is UNIDROIT, an inter-governmental organisation responsible solely to its Member States, which operates on the basis of consensus. The UNIDROIT Principles are an example of 'rules of law' that are 'generally accepted on an international level'. Moreover, the UNIDROIT Principles expressly provide that parties may designate them to govern their contract and suggest choice of law clauses to that end (see the footnote to the UNIDROIT Principles' Preamble and the Model Clauses for the Use of the UNIDROIT Principles of International Commercial Contracts)'.

99 Significantly enough,, however, even the most vehement critics of the provision concede that their opposition would have been much weaker if at stake was only the possibility to choose as the lex contractus the UNIDROIT Principles: so expressly, e.g., Mankowski, 2017: 'If it was only for the UNIDROIT Principles the battle for a choice of non-state law would hardly be so heated.

100 So expressly Article 28(1) of the 1985 UNCITRAL Model Law on International Commercial Arbitration.

References

1. Walch, A. (2019). In code(rs) we trust: Software developers as fiduciaries in public blockchains. In P. Hacker et al. (Eds.), *Regulating blockchain: Techno-social and legal challenges* (pp.58–82). Oxford. https://doi.org/10.1093/oso/9780198842187.003.0004
2. Frantz, C. K., & Nowostawski, M. (2016). From institutions to code: Towards automated generation of smart contracts. *IEEE 1st International Workshops on Foundations and Applications of Self Systems (FAS*W)*, *53*, 210–215. https://doi.org/10.1109/FAS-W.2016.53
3. Easterbrook, F. H. (1996). Cyberspace and the Law of the Horse. *University of Chicago Legal Forum*, *1996*(1), Article 7. https://chicagounbound.uchicago.edu/uclf/vol1996/iss1/7/
4. Lessig, L. (1996). The law of the horse: What cyberlaw might teach. *Harvard Law Review*, *113*, 501–546. https://cyber.harvard.edu/works/lessig/finalhls.pdf
5. Epstein, R. A. (1995). *Simple rules for a complex world*. Harvard University Press.
6. Katz, D. M. (2013). Quantitative legal prediction — Or — How I learned to stop worrying and start preparing for the data-driven future of the legal services industry. *Emory Law Journal, 4*(6), 909–936. https://scholarlyy commons.law.emory.edu/elj/vol62/iss4/6
7. Jaccard, G. O. B. (2017). Smart contracts and the role of law. *Jusletter IT,* (22). https://lawded.ch/wp-content/uploads/2019/07/x.pdf
8. Szczerbowski, J. (2017). Place of smart contracts in civil law. A few comments on form and interpretation. *Law & Society: Private Law — Contracts eJournal*. https://www.semanticscholar.org/paper/Place-of-Smart-Cono tracts-in-Civil-Law.-A-Few-on-and-Szczerbowski/cddc80a1e54765d698e13cd242512ec73fa97cdb
9. Surden, H. (2012). Computable Contracts. *U.C. Davis Law Review, 46,* 629-700. https://lawreview.law.ucdavis.edu/issues/46/2/Articles/46-2_Surden.pdf
10. Ho, H. M., & Law, J. (2021). Singapore. In M. S. Sackheim, & N. A. Howell (Eds.) The virtual currency regulation review (4th ed., pp. 233–244). https://www.sidley.com/-/media/publications/vcrr-edition-4--singapore.pdf?la=en
11. Druck, J. A. (2018). Smart contracts are neither smart nor contract. *Banking & financial services policy report*, *37*(10), 5–9.
12. Schrey, J., & Thalhofer, T. (2017). Rechtliche Aspekte der Blockchain [Legal issues of blockchain]. *Neue Juristische Wochenschrifft*, *70*(20), 1431–1436.
13. Levy, K. E. C. (2017). Book-smart, not street-smart: Blockchain-based smart contracts and the social workings of law. *Engaging Science, Technology, and Society*, *3*, 1–15. https://doi.org/10.17351/ests2017.107
14. Kõlvart, M., Poola, M., & Rull, A. (2016). Smart contracts. In T. Kerikmäe, A. Rull (Eds.) *The future of law and e-technologies*. Springer. https://doi.org/10.1007/978-3-319-26896-5_7
15. Baptista, L. O. (1995). The UNIDROIT principles for international commercial law project: Aspects of international private law. *Tulane Law Review*, *69*(5), Article 1209. https://www.tulanelawreview.org/pub/volume69/issue5/the-unidroit-principles-for-international-commercial-law-project
16. Kaulartz, M., & Heckmann, J. (2016). Smart Contracts — Anwendungen der Blockchain-Technologie [Smart Contracts — Application of blockchain technology]. *Computer und Recht*, *32*(9), 618–624. https://doi.org/10.9785/cr-2016-0923
17. Spindler, G. & Woebbeking, M. K. (2019). Smart Contracts und Verbraucherschutz [Smart contracts und consumer protection]. In T. H. Braegelmann, & M. Kaulartz (Eds.) *Rechtshandbuch Smart Contracts*. C.H. Beck.
18. Bonell, M. J. (2018). The law governing international commercial contracts and the actual role of the UNIDROIT Principles. *Uniform Law Review*, *23*(1), 15–41. https://doi.org/10.1093/ulr/uny001
19. Szabo, N. (1996). Smart contracts: Building blocks for digital markets. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
20. Reusch, P., & Weidner, N. M. (2018). *Future Law: Blockchain, industrie 4.0, Internet of things, robotic*. Fachmedien Recht und Wirtschaft.
21. Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Law Tech Review*, (1), 305–341.

22. Dale, R. (2010). Classical approaches to natural language processing. In N. Indurkhya, & F. J. Damerau (Eds.) *Handbook of natural language processing* (2d ed., pp. 6–21). Chapman & Hall. https://doi.org/10.1201/9781420085938
23. Cohney, S., Hoffman, D., Sklaroff, J., & Wishnick, D. (2019). Coin-operated capitalism. *Columbia Law Review, 119*(3), 591–676. https://columbialawreview.org/content/coin-operated-capitalism/
24. Nzuva, S. (2019). Smart contracts implementation, applications, benefits, and limitations. *Journal of Information Engineering and Applications*, *9*(5), 63–75. https://doi.org/10.7176/JIEA
25. Blemus, S. (2018). Law and blockchain: A legal perspective on current regulatory trends worldwide. *Revue Trimestrielle de Droit Financier*, (4), 1–15.
26. Kiviat, T. I. (2015). Beyond Bitcoin: Issues in regulating blockchain transactions. *Duke Law Journal*, *65*(3), 569–608. https://scholarship.law.duke.edu/dlj/vol65/iss3/4
27. Schroeder, J. L. (2016). Bitcoin and the uniform commercial code. *University of Miami Business Law Review*, *24*(3), 1–79. https://repository.law.miami.edu/umblr/vol24/iss3/3/
28. Fairfield, J. A. T. (2015). Bitproperty. *Southern California Law Review*, *88*(4), 805–874. https://southerncalifornialawreview.com/2015/05/02/bitproperty-article-by-joshua-a-t-fairfield/
29. Ricks, Val D. (1999). In defense of mutuality of obligation: Why "both should be bound, or neither. *Nebraska Law Review*, *78*(3), 491–549. https://digitalcommons.unl.edu/nlr/vol78/iss3/2/
30. Werbach, K, & Cornell, N. (2017). Contracts Ex Machina. *Duke Law Journal*, *67*(2), 313–382. https://scholarship.law.duke.edu/dlj/vol67/iss2/2
31. Savelyev, A. (2017). Contract law 2.0: 'Smart 'contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*(2), 116–134. https://doi.org/10.1080/13600834.2017.1301036
32. Surden, H. (2014). Machine Learning and Law. *Washington Law Review, 89*(1),87–115. https://digitalcommons.law.uw.edu/wlr/vol89/iss1/5/
33. Kristy, M. A. C., & Jing, Z. (2013). Public policy violation under New York Convention. Mimbar Hukum, 25(1), 139–150. https://jurnal.ugm.ac.id/jmh/article/view/16105
34. Frantz, C. K., & Nowostawski, M. (2016). From institutions to code: Towards automated generation of smart contracts. In 2016 IEEE 1st International Workshops on Foundations and Applications of Self Systems (FAS*W) (pp. 210–215). Piscataway. https://doi.org/10.1109/FAS-W.2016.53
35. Coote, B. (1988). The essence of contract. Pert 1. *Journal of Contract Law*, *1*(2), 91–112.
36. Cons, G. M., & Hernández, G. M. A. (2019). Importance of a legal framework in smart contracts. Sinteza 2019 — International Scientific Conference on Information Technology and Data Related Research, 2019, 603–608. https://doi.org/10.15308/Sinteza-2019-603-608
37. Goode, R. (2005). Rule, practice, and pragmatism in commercial law. *International and Comparative Law Quarterly*, *54*(3), 539–562. https://doi.org/10.1093/iclq/lei017
38. Mankowski, P. (2017). Article 3 of the Hague Principles: The final breakthrough for the choice of non-State law? *Uniform Law Review*, *22*(2), 369–394. https://doi.org/10.1093/ulr/unx016

Information about the author:

Gabriel R. De En Goh — Ph.D., International Arbitrator, Legal Counsel, Fellow, The College of Law, Sydney, Australia.
roydeengoh@gmail.com

Сведения об авторе:

Де Эн Го Г. Р. — Ph.D., Международный Арбитр, Юрисконсульт, Научный сотрудник Школы права, Сидней, Австралия.
roydeengoh@gmail.com

https://doi.org/10.38044/2686-9136-2022-3-4-71-88

ARTICLES

DATA-SHARING AS A QUID PRO QUO OF CO-REGULATION IN THE EU

Mark L. Entin,[1]* Ekaterina G. Entina[2], Dmitriy V. Galushko[3]

[1]Moscow State Institute of International Relations (MGIMO-University)
76, ave. Vernadsky, Moscow, Russia, 119454

[2]Higher School of Economics (HSE University)
3, Bolshoy Trekhsvyatitelskiy Pereulok, Moscow, Russia, 109028

[3]Financial University
49, Leningradsky Prospect, Moscow, Russia, 125993

Abstract

The paper focuses on the defining of the co-regulation of national and supranational legal regimes' features of data-sharing in the digital platforms' functioning on the example of the EU's practice with a special attention to the disintegration process of Brexit. Data-sharing is one of the most appropriate spheres to demonstrate specific traits of digital platforms — the cross-border character of their operation. This demands quid pro quo interaction of the national and supranational regulatory regimes, filling the gap associated with the lack of international regulation and the inability to harmonize law. We begin with the theoretical characterization of information and personal data, the right to privacy, and classifications of interventions in private life. The EU has been chosen as an example, acting as a flagship of interaction of national and supranational legal orders in relation to the co-regulation of cross-border data-sharing in digital platforms. Interaction of the EU on the principle of quid pro quo, based on the practice of making decisions on adequacy, is considered in the context of Brexit and the relevant law-making practice of the UK. The discussion is complemented by examples of similar EU relations with South Korea and the United States. Based on the analysis, the authors conclude that the EU supranational legal order has a high degree of influence on the national legislation of third countries, which contributes to the constant development of regulation in the sphere and the strengthening of international integration.

Keywords

data-sharing, personal data, privacy, publicity, European Union, Great Britain, GDPR, Brexit

Conflict of interest	The authors declare no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Entin, M. L., Entina, E. G., & Galushko, D. V. (2022). Data-sharing as a quid pro quo of co-regulation in the EU. *Digital Law Journal, 3*(4), 71–88. https://doi.org/10.38044/2686-9136-2022-3-4-71-88

* Corresponding author

Submitted: 18 Sep. 2022, accepted: 10 Nov. 2022, published: 31 Dec. 2022

СТАТЬИ

ОБМЕН ДАННЫМИ КАК QUID PRO QUO СОВМЕСТНОГО РЕГУЛИРОВАНИЯ В ЕС

М.Л. Энтин[1,*], Е.Г. Энтина[2], Д.В. Галушко[3]

[1]Московский государственный институт международных отношений (МГИМО-Университет) МИД России
119454, Россия, Москва, просп. Вернадского, 76

[2]Национальный исследовательский университет «Высшая школа экономики»
109028, Россия, Москва, Большой Трехсвятительский пер., 3

[3]Финансовый университет при Правительстве Российской Федерации
125167, Россия, Москва, просп. Ленинградский, д. 49/2

Аннотация

Статья посвящена определению особенностей совместного регулирования национальными и наднациональными правовыми режимами обмена данными в функционировании цифровых платформ на примере практики ЕС с особым вниманием к дезинтеграционному процессу Брекзита. Обмен данными является одной из наиболее подходящих сфер для демонстрации специфических черт цифровых платформ — трансграничного характера их функционирования. Данный процесс требует взаимодействия национальных и наднациональных режимов регулирования по принципу quid pro quo, заполняя пробелы, связанные с отсутствием международного регулирования и неспособностью гармонизировать соответствующее право. Авторы начинают исследование с теоретической характеристики информации и персональных данных, права на неприкосновенность частной жизни и классификации вмешательств в нее. В качестве примера был выбран опыт ЕС, выступающего в качестве флагмана взаимодействия национального и наднационального правопорядков в отношении совместного регулирования трансграничного обмена данными в рамках цифровых платформ. Взаимодействие ЕС по принципу quid pro quo, основанное на практике принятия решений об адекватности, рассматривается в контексте Брекзита и соответствующей правотворческой практики Великобритании. Обсуждение дополняется примерами аналогичных отношений ЕС с Южной Кореей и Соединенными Штатами. На основе проведённого анализа авторы приходят к выводу о высокой степени влияния наднационального правопорядка ЕС на национальное законодательство третьих стран, что способствует постоянному развитию регулирования в рассматриваемой сфере и укреплению международной интеграции.

Ключевые слова

обмен данными, персональные данные, конфиденциальность, публичность, Европейский союз, Великобритания, Брекзит

Конфликт интересов	Авторы сообщают об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.

Для цитирования Энтин, М. Л., Энтина, Е. Г., Галушко, Д. В. (2022). Обмен данными как quid pro quo совместного регулирования в ЕС. *Цифровое право, 3*(4), 71–88. https://doi.org/10.38044/2686-9136-2022-3-4-71-88

* Автор, ответственный за переписку

Поступила: 18.09.2022, принята в печать: 10.11.2022, опубликована: 31.12.2022

Introduction

The phrase *'quid pro quo'* can be described as an exchange of something for something. In the context of the functioning of digital platforms, it usually refers to an exchange of goods and services for personal data or other information products in place of compensation (Walker, 2015). Significant progress in the development of digital platforms — namely the introduction of information and telecommunication technologies and the associated increase in the volume and directions of using the information in various spheres of public life, as well as its transmission by the latest communication means — have significantly expanded the possibilities for collecting, storing, and processing information in relation to individual citizens. A traditional firm can only collect data on its own customers, but a digital platform can access a vast amount of data related to all sellers and buyers on multiple sides of its platform (Eisenmann et al., 2011).

Activity in the formation of automated databases, processing, and dissemination of information about persons without their knowledge has led to the emergence of a global problem, in particular, the scale (in both time and space) of the problem of information security of people, society, and the state for the protection of personal data. The data that fuels digital platforms heightens these dynamics in a way that is qualitatively and quantitatively different from the way it effects conventional markets (Kira et al., 2021); that is, the problem of protecting the interests of the individual in the information sphere is also the problem of protecting personal data, which concerns all spheres of human activity, society, and the state. The well-being of both the individual and the state depends on understanding the importance and necessity of creating a mechanism to protect personal data.

Globalized trade and increased cross-border transactions present interesting legal implications for the ability of public and private subjects to control and protect data. Digital platforms have made it possible for transactions to be concluded beyond national borders.[1] Consequently, the development of digital platforms has led to a huge growth in the volume of cross-border transmitted personal data, which acts as a new currency in the *quid pro quo* interaction of national and supranational regulatory regimes, particularly their co-regulation at the normative and institutional levels.

The globalization of trade in digital data and services has not been accompanied by a general harmonization of Internet law (Voss, 2019), nor a true convergence of data protection and data privacy laws (Voss, 2020). Consequently, now it is possible to envisage an avalanche of new laws and regulations attempting to govern and impose order on a dizzying array of tech developments.[2] It is expected that international authorities will make full use of their new powers in order to apply

[1] Serzo, A. L. O. (2020). *Cross-border data regulation for digital platforms: Data privacy and security.* [Discussion Papers DP 2020-47]. Philippine Institute for Development Studies.

[2] Tene, O. (2022, January 3). The year ahead: Privacy developments in 2022. *Goodwin*. https://www.goodwinprivacyblog.com/2022/01/03/the-year-ahead-privacy-developments-in-2022/

and enforce their respective data protection legislation in the near future.[3] The headliner legislator is the European Union, which is recognized as the creator of the global standard for 'best practice' in data governance and co-regulation between national and supranational legislators.[4] Examining the relationship between national legal regimes and supranational data protection regulation is of special interest in the context of the unique process of Great Britain's withdrawal from the European Union — Brexit.

Methodology

The methodological basis of this article is a complex of general scientific and special methods, the expediency of which is determined by the specifics of the object of research. A systematic approach and structural and functional analysis were used in the course of this study to reveal the essence and genesis of data-sharing, its structure and functions in modern society, and the role of digital platforms. When studying the mechanisms for legal support of data sharing at national and supranational levels, a system-structural and dialectical method of scientific knowledge of legal processes and phenomena was used, which manifested itself, in particular, in the widespread use of certain categories of dialectics. The application of the formal-logical method made it possible to carry out a logical, grammatical, and morphological analysis of the existing legal norms. The use of the comparative method made it possible to study the compliance of national legislation with European standards in this area, as well as to analyze the process of transfer and protection of personal data between the European Union and the United Kingdom after Brexit.

Results

From the outset, it should be mentioned that the term 'information' entered scientific circulation long before the rapid development of communication tools, digital platforms, and data conversion, as well as transmission technologies based on it. The emergence of branches of science and technology directly related to them have turned it into an iconic symbol of the modern era. There are many definitions of information as a result of scientific discussion and various approaches to the interpretation of this concept. The original concept of 'information' was associated exclusively with communicative activities in society (Nitecki, 1985). It was found that information is the highest, most complex result of an orderly reflection in the form of messages, knowledge, and information about nature, society, and objective reality in general, covering all spheres of human activity used in the process of communication, management, production, cognition, creativity, upbringing, education, etc. This makes it possible to pay attention to the managerial nature of the information. Information is seen as the unity of updating diversity and as its limitation. The main function of information is to convey an idea (to inform) about an object, while reflecting its properties.

One kind of information is personal information that reflects both the individuality of a person and their universal biological and social properties. Personal information reflects human diversity: the individuality of each person as a carrier of unique elements of physical, physiological, mental, economic, cultural, and social identity. The defining feature of personal information is its

[3] Gibson Dunn. (2022, January 31). *International cybersecurity and data privacy outlook and review — 2022*. https://www.gibsondunn.com/international-cybersecurity-and-data-privacy-outlook-and-review-2022/

[4] Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business*. https://www.privacylaws.com/reports-gateway/articles/int169/s_int169dplaws2021/

individualized nature and the ability to identify a specific person using certain criteria. During such identification, the process of personifying certain information takes place: that is, linking them to a specific person. Identifying information makes it possible to identify a person, either directly or with the help of other factors. Information (both documented and oral) is a form of reflection of the biological and social identity, as well as the individuality of each person (Mingers & Standing, 2018).

To refer to information about an individual that has already undergone certain processing, has been recorded and ordered in a certain medium, and is suitable for automated processing, the term 'personal data' is used (Lat. *personalitas* — personality).

The unlawful collection, use, and dissemination of personal information damages the image of the individual. This does not only apply to biographical data, such as a person's surname, name, patronymic, date of birth, place of birth, nationality, religious, political, or philosophical beliefs, education, place of study and work, information about marital status, presence of children, or attitude to military service. Personal information includes information about a person's material and financial condition (bank accounts, payments in them, real estate and movable property, property rights), health status, personal relationships of a private nature, and a lot of other information in material form in various areas of public life that are created, collected, stored, distributed, and used in other ways, both with the consent of the data subject, and without their knowledge. This information allows society to evaluate a person as an individual, to form their reputation (Lat. "reputatio" — evaluation).[5]

Protecting the confidentiality of personal information has become relevant during the emergence and widespread risks to life, health, reputation, and human well-being due to the illegal collection and use of personal information — that is, from unwanted intrusion into the internal sphere of human life, which is protected by the right to respect for private life (Beck et al., 2016).

If half a century ago it was necessary to expend considerable effort to obtain information about a person, the current level of information technology development — in particular, the functioning of digital platforms — makes it possible to process data on thousands of people in a matter of seconds without incurring excessive costs. The combination of inaccurate or outdated personal data will create a misleading impression of an individual.

The capabilities of digital platforms that allow the collection and processing of personal information are constantly and rapidly expanding. Technologies are improving, and their cost is decreasing. Even with conventional information collection technologies, a significant amount of personal information is constantly collected. For example, any payment transaction on a digital platform, whether it is a purchase, sale, or investment, creates a collection of personal data. Subsequently, digital platforms can use such information both for commercial purposes and for reporting to the fiscal authorities of the state.[6]

It should be noted that, from the point of view of a person's security, that different kinds of personal information have different degrees of importance per individual, which is determined by the level of risk of harm. Given the threat of poor perception by others, discrimination on a certain basis, or other illegal use of personal information, its potential to create 'vulnerability' for a person must be foreseen. To take into account the interests of the individual and their subjective attitude to information, which cannot be fully covered in generalized regulatory prescriptions, a voluminous

[5] Sierra, C. & Debenham, J. (2009). *Information-based reputation*. Proceedings of the first international conference on reputation: Theory and technology — ICORE 09, 5 – 19. https://opus.lib.uts.edu.au/handle/10453/10892

[6] OECD. (2019). *The role of digital platforms in the collection of VAT/GST on online sales.* www.oecd.org/tax/consumption/the-role-of-digital-platforms-in-the-collection-of-vat-gst-on-online-sales.pdf

list of data must be legally classified as 'sensitive data' (including that concerning racial or ethnic origin or nationality, political views, religious or philosophical beliefs, membership in trade unions or public organizations, information related to health or the provision of health care, family and personal relationships of a private or sexual nature, criminal acts or illegal behavior), and people must be granted the right to independently determine the boundaries of the circulation of their personal information in society. This creates a territorial space in which a person can control the boundaries of their individuality. To effectively protect this space, a person must have the right to define these boundaries — that is, to determine what personal information can be transferred, for what purposes, to what extent, and to what recipients.

This approach is due to the fact that only the person to whom the personal information relates can assess the likely risk of misuse of such information. This is the basis of the nature of the right to privacy of personal information and the awareness of such as belonging to the 'private sphere' of human life. Legal doctrine uses the term 'privacy' to refer to this legal institution. It characterizes the qualitative state of the object, which follows from its belonging to the 'private sphere' of human life. In addition, this term is immediately associated with what belongs directly to a private person and is inaccessible to the public as a 'private matter', as opposed to a 'public' one.

The first concept of the right to privacy passed judicial testing in the United States. In the practice of American courts, cases of commercial use of the personal characteristics of individuals, such as appearance, name, and voice, have often been considered. Such cases concerning human rights violations have often been accompanied by violations of property rights. American courts have recognized these individual personality traits, which were encroached upon by other persons, as an object of protection of property interest. The traditional Western idea of the right to privacy originates from the right to the inviolability of homeownership, and the Western doctrine of privacy is territorial in nature, since it protects the personal living space of a person.[7]

After studying the precedents created by US courts when considering cases regarding interference with a person's private life, an American lawyer, William L. Prosser (1964), proposed the following classification: disclosure of facts relating to private life, reporting false information about a person, misuse of images of a person's appearance, voice, and, finally, physical harassment (Prosser, 1964).

The Swedish researcher Stromholm proposed his own classification of interventions in private life. Having singled out 14 types of unlawful attacks on privacy, he grouped them into three groups, taking into account the direction of the offenders' actions:

1) actions aimed at invading the private sphere of a person's life — an illegal search, sending letters with insults, harassment by phone calls

2) illegal actions, thanks to which violators obtain information about the private life of a person: wiretapping, interception of correspondence, etc.

3) dissemination or other use of information about a person's private life: publication of information about a person's private life in the press, the use of a person's name and appearance (Resta, 2011).

Since it is the right of a person to the privacy of personal information that becomes the object of legal protection, this type of privacy is called 'informational privacy'. This kind of privacy also has a territorial dimension, since information flows circulate in a certain space. A person is the main source of information generated within their own living space and is a consumer of information that comes to them from the outside, particularly within digital platforms.

[7] Solove, D. J. (2006). A brief history of information privacy law. In *Proskauer on privacy. PLI.* https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications

It is also necessary to distinguish between the spheres in which the social activity of a person is realized. This makes it possible to break down the general problem of protecting human privacy into sectors that require separate legislative regulation. According to this criteria, four types of privacy can be distinguished:

1) informational privacy, which covers the rules for the collection and processing of personal data

2) bodily (physical) privacy, relating to the protection of the physical integrity of a person from coercive procedures, such as drug testing, etc.

3) communication privacy, covering the security and confidentiality of postal items, telephone conversations, electronic correspondence, and other forms of communication

4) territorial inviolability, with regard to the establishment of a legal framework for protection against interference in the family sphere, other environments, the workplace, or a vehicle (Resta, 2011).

This classification makes it possible to understand the complexity and interconnectedness of the legal regulation of data-sharing, being a key to protecting the privacy of personal information. At the same time, digital platforms act as carriers of such data. The rapid development of digital platforms, in which messages are transmitted in digital form, does not set up the possibility, technically or normatively, to distinguish between where communication privacy ends and personal data confidentiality begins. This makes the legal developments in the sphere quite complicated. Nevertheless, legislative measures continue to develop at speed all over the world.[8]

In addition, the problem of ensuring the right to privacy of users of digital platforms is complicated by the extraterritorial nature of information exchange. Digital platforms make it possible to establish direct contact between a human data subject under the jurisdiction of one state and other subjects of information exchange that may be located on the territory of other states. In the era of digital platforms and Big Data, legal relations arise at the intersection of jurisdictions, since the personal data of any person (a citizen of any state) can be processed by business entities in foreign jurisdictions. Ensuring the operation of national provisions — and therefore guaranteeing an adequate level of privacy protection for its citizens in this environment — becomes problematic for the state. At the same time, the creation by national governments of artificial obstacles to the free cross-border circulation of personal information will negatively affect international cooperation in many areas. Understanding this problem prompted the international community to develop cooperation in order to ensure the continuity of information exchange, which led to the creation of a set of international norms and principles that are covered by the international legal institution for the protection of the confidentiality of personal information.

Thus, in protecting the right to privacy of personal information, there is a focus on ensuring the freedom of the individual to determine the spatial and temporal framework of information contact with other subjects, as well as the controllability of the circulation of personal information in society, which is important for maintaining the autonomy of the individual, as well as protecting the private sphere of their life. That is the case for the European Union, where the issue of personal data protection is often considered in the context of the protection of fundamental human rights guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union. This protection afforded to the data of European citizens extends beyond the borders of the Union, especially when data is transferred outside European territory. More specifically, the transfer of personal data outside the

[8] DataGuidance. (2022, June 2022). *Keeping up to date with global privacy updates.* https://www.dataguidance.com/resource/keeping-date-global-privacy-updates

European Union is only permitted if the protection of data offered by the country receiving the data is considered 'adequate' by the EU. Therefore, such a state must provide guarantees equivalent to those provided by the Union's law.

EU data protection law provides for the unimpeded flow of personal data in the European Economic Area (hereinafter referred to as the EEA), which includes the EU member states, Norway, Iceland, and Liechtenstein. The transfer of personal data to non-member countries is only permitted in limited cases due to the fact that this issue acts as an element of the digital sovereignty of the EU.

As the European Union is lagging behind the United States and China in certain areas of information and communication technology development, concern over the dominance of digital platforms and security issues has naturally led to increased attention being paid to the problem of the EU establishing its own 'digital' sovereignty.[9] Ursula von der Leyen, President of the European Commission, has specifically pointed out this need.[10] The need to "establish digital sovereignty as the leitmotif of European digital policy" was also expressed by the German side in its EU Council Presidency program of July 2020.[11] In general, calls are increasingly being made in the EU to build a European cloud and information infrastructure for strengthening European digital sovereignty and addressing the fact that, today, the cloud and IT market is almost exclusively dominated by non-European digital platforms — with potentially detrimental consequences for the security and rights of EU citizens (Martirosjan, 2021). Later on the French Presidency[12] of the Council of the European Union has picked up the baton in this regard, paying the most serious attention to the protection of personal data.[13]

The principles of the EU Charter on personal data are also embodied in the Lisbon Treaty of 2009. On November 4, 2010, the European Commission published a strategy for strengthening data protection at the European level.[14] In January of 2012, the European Commission approved a comprehensive reform plan, including the need to replace the Directive with an EU Regulation that would establish uniform requirements across the EU.[15] In 2016, the same year the Brexit referendum was held, the EU data protection law saw the most significant change since the introduction of the Data Protection Directive in 1995 through the adoption of the General Regulation on Data Protection Regulation

[9] Gueham, F. (2017). Digital sovereignty — Steps towards a new system of internet governance. *Fondapol.org.* https://www.fondapol.org/en/study/digital-sovereignty-steps-towards-a-new-system-of-internet-governance/

[10] European Commission. (2019). *Political guidelines for the next European Commission 2019–2024.* https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf

[11] Hasanova, A. (2021). Evropejskij podhod k «tehnologicheskomu suverenitetu» [European approach to "technological sovereignty"]. *RIAC*. https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/evropeyskiy-podkhod-k-tekhnologicheskomu-suverenitetu/

[12] French Presidency of the council of the European Union. (n.d.). *Personal data*. Retrieved August 4, 2022, from https://presidence-francaise.consilium.europa.eu/en/personal-data/

[13] Council of the European Union. (2021). *Council Decision on the conclusion, on behalf of the Union, of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, and of the Agreement between the European Union and the United Kingdom of Great Britain and Northern Ireland concerning security procedures for exchanging and protecting classified information.* https://data.consilium.europa.eu/doc/document/ST-5022-2021-REV-3/en/pdf

[14] European Commission. (2010). *European Commission sets out strategy to strengthen EU data protection rules.* https://ec.europa.eu/commission/presscorner/detail/en/IP_10_1462

[15] European Commission. (2012). *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses.* https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46

(GDPR),[16] the first EU legal instrument regulating the protection and free flow of personal data that is directly applicable in all EU member states.

The GDPR aims to protect the regulation on personal data, which is set out in the EU Charter and the Treaty on the Functioning of the European Union. The GDPR's substantive scope concerns automatic and non-automatic data processing, with the exception of the processing of data by EU institutions, which is regulated by another regulation. The application of the GDPR has several justified exceptions: criminal prosecution procedures, security provisions under the Treaty on the Functioning of the European Union, scope of data processing that goes beyond EU law, and the processing of personal data of natural persons for exclusively private purposes ("private processing") (Voigt & Von dem Bussche, 2017).

The GDPR's principles provide that personal data:

- is processed lawfully, fairly, and transparently ("legal, fair, and transparent")
- is collected for specific, explicit, and legitimate purposes ("limitation for purposes")
- must be adequate, appropriate (for the purposes of processing), and limited solely to the purposes for which they are processed ("data minimization")
- processed accurately ("accuracy")
- stored in a form that allows the identification of the data subject no longer than is necessary for the purposes of the processing ("storage limit")
- processed in such a way as to ensure adequate security of personal data ("integrity and confidentiality")

It should be noted that some of the GDPR's principles have been elaborated and improved on the basis of the jurisprudence of the EU Court of Justice.

According to Chapter V of the GDPR, there are several legal bases that allow the transfer of data from the EU to non-EU countries. One of the most convenient ways to seamlessly transfer data from the EU to a state that is not a member of the Union is to obtain a decision from the European Commission on adequacy. The transfer of data to a state that is not a member of the EU, but which has an adequacy decision, does not require additional legal grounds for cross-border transfer (Article 45(1) of the GDPR). The procedure and requirements for the adequacy decision are qualified and specified in the EU decision on adequacy.[17] An adequacy decision is considered a proper basis for cross-border transfer for four years after it has been made and/or successfully reviewed, or unless it is challenged before the Court of Justice (for example, the *Privacy Shield case*).

In practice, the European Commission issues an adequacy decision based on an opinion issued by the European Data Protection Board (EDPB) in accordance with Article 70(1)(s) of the GDPR and Articles 2 and 12 of the EDPB Rules of Procedure.[18] This function was previously performed by the Working Party on Article 29 (hereinafter — 29WP). The 29WP produced 12 adequacy decisions. Prior to the adoption of the first adequacy decision in 1998, the 29WP published a special Working Paper that covered all the

---

[16] European Union. (2016b). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).* https://eur-lex.europa.eu/eli/reg/2016/679/oj

[17] European Commission. (2018). *Working document on Adequacy Referential (wp254rev.01).* https://ec.europa.eu/newsroom/article29/items/614108

[18] EDPB. (2018, May 25). *European Data Protection Board Rules of Procedure*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_rop_version_6_adopted_20200129_en.pdf

important issues related to adequacy decisions.[19] Although 29WP has been superseded by the EDPB (Article 94(2) of the GDPR), this Working Paper remains a solid step-by-step plan for assessing the adequacy of protection afforded by a non-member country containing practical steps to be taken by the applicant country concerned in order to obtain an adequacy decision from the EU side.

When deciding on adequacy, the EDPB and the European Commission take into account, inter alia, the following circumstances:

- due diligence on data protection and the rule of law in a broad sense (including other international obligations, such as those within the EEA)
- access of the data subject to effective law enforcement and judicial protection
- the existence of an independent and effective supervisory body
- the jurisprudence of the EU Court of Justice and the European Court of Human Rights on matters related to privacy
- compliance with 29WP and EDPB guidelines
- recent and future changes to the General Regulations (for example, the decision on the Privacy Shield was made subject to the GDPR's entry into force)

In general, the participation of the European Union in dialogue and, if necessary, negotiations with non-member countries (including EU strategic partners and the countries of the European Neighborhood Policy) and international organizations (such as the Council of Europe, the Organization for Economic Cooperation and Development, United Nations) tends to promote highly compatible data protection standards worldwide.[20] The EU acts as a supranational entity that sets global rules in a number of areas of regulation: antitrust, privacy, health (through chemicals regulation), environmental protection and food safety. The area of privacy protection, where Europe sets the tone, is central, because EU legislation in this area affects the laws of territories outside its borders (Bradford, 2012). Thus, unsurprisingly, the issue of data-sharing has acquired particular relevance in connection with disintegration reflections — the UK's withdrawal from the European Union.

Cross-border data-sharing after Brexit is no longer free but must be supported by a specific legal instrument or mechanism since the United Kingdom is no longer subject to EU law. However, it seems that the importance of such a decision cannot be truly appreciated without highlighting the crucial role that data-sharing plays in terms of trade and economic relations, as well as other forms of non-commercial cooperation between the UK and the EU. That is why some researchers note that "data protection could potentially be among the problems that could 'make' or 'hinder' a possibly successful Brexit" (De Hert & Papakonstantinou, 2017).

The months leading up to the 2016 Brexit referendum and the first few months afterwards were characterized by lively discussions about the advantages and disadvantages of the UK leaving the EU (Nicolaïdis, 2017). A plethora of figures and data describing current trade relations with EU and non-EU countries, as well as speculation about potential future UK relations, have been used to substantiate sometimes quite opposing opinions and points of view. However, data regarding data-sharing between the EU and the United Kingdom clearly points to a deeply intertwined architecture of trade and economic relations between the parties, as well as other forms of cooperation in many areas

[19] European Commission. (1998). *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* [Working Document]. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf

[20] Shadrin, S. A. (2019). *Pravovoe regulirovanie zashhity personal'nyh dannyh v Evropejskom Sojuze: Genezis i perspektivy razvitija* [Legal regulation of personal data protection in the European Union: genesis and development prospects: Ph.D. dissertation] [Unpublished doctoral dissertation]. Kazan.

that are heavily dependent on the exchange of personal data, which will be damaged in the event of a sudden impediment to such cross-border exchange.[21]

In 2018, the UK, then an EU member state, updated its legislation to GDPR standards. The EU's GDPR came into force on May 23, 2018, and the UK Data Protection Act of 2018 was passed on the same day. Still, on January 31, 2020, Great Britain left the EU and entered an 11-month transition period, during which EU legislation continued to fully apply to the territory of the country.

The 2018 Act firstly supplemented the GDPR in areas where EU regulation allowed member states to adopt additional regulations, such as on conditions for processing special categories of data (Article 9 of the GDPR) or on derogations from the rights of data subjects (Article 23 of the GDPR). Secondly, it applied a limited set of GDPR rules to rare cases of data processing that went beyond its scope — for example, to government bodies that process personal data in unregistered documents, as well as bodies other than law enforcement or intelligence services that process data for national security or defense purposes. Thirdly, the 2018 Act implemented EU Directive 2016/680 in UK legislation, which regulates the processing of personal data by law enforcement agencies. Fourthly, it created a legal framework for the protection of personal data processed by intelligence agencies.

This legal regime was in effect until Exit Day. The European Union (Withdrawal) Act of 2018 provides that, at the end of the transitional period, EU law in force on December 31, 2020 — including regulations such as the GDPR and European Commission adequacy decisions — will be incorporated into UK law as "EU retained law".[22] Thus, the GDPR and its principles have been and remain part of UK law. The British Parliament has published explanatory notes confirming that the 2018 Act and the GDPR apply substantially the same standards for most data processing in the UK and are sufficient to create a clear and consistent data protection regime.[23]

Based on this, UK businesses were required to comply with both the GDPR and the 2018 Act during the transition period, and to comply with the requirements of UK law upon its completion.

In October of 2018, the UK regulator published its first enforcement notice under Section 149 of the 2018 Act against AggregateIQ Services Ltd. In 2020, a notice of intent to fine the Marriott International hotel network was published (with a fine of £18.4m) due to a data breach.[24] The first fine was imposed on December 20, 2019, on the Doorstep Dispensaree pharmaceutical company. The fine was £275,000.[25] It should be noted that the GDPR and the 2018 Act affect digital platforms in the UK in a similar way as in the European Union. At the same time, companies in the UK are having difficulty meeting the requirements of the GDPR. Since the implementation of GDPR, the UK has reported 40,026 personal data breach notifications, with 8,355 reported in 2020, and 9,490 in 2021 — a 13.6% increase in one year.[26]

21 UK Government. (2020). *Explanatory framework for adequacy discussions — Section A: Covering note*. https://www.gov.uk/government/publications/explanatory-framework-for-adequacy-discussions

22 UK Legislation. (2018). *European Union (Withdrawal) Act 2018*. https://www.legislation.gov.uk/ukpga/2018/16/contents/enacted

23 UK Parliament. (2018). *Data Protection Bill Explanatory Notes*. https://publications.parliament.uk/pa/bills/lbill/2017-2019/0104/18104en01.htm

24 Information Commissioner's Office. (2020). *ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure*. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/

25 Information Commissioner's Office. (2020). *Doorstop Dispensaree Ltd monetary penalty notice*. https://ico.org.uk/action-weve-taken/enforcement/doorstep-dispensaree-ltd-mpn/

26 Weston, S. (2022, January 18). European data regulators issued €1.1 billion in GDPR fines in 2021. *ITPro*. https://www.itpro.co.uk/policy-legislation/general-data-protection-regulation-gdpr/362000/european-data-regulators-issued

In general, British legislative changes have been aimed at the sovereignization of the legal regulation of the sphere in question. The Data Protection Act of 2018 temporarily allowed the transfer of data to countries that received adequacy decisions from the European Commission before the EU exit day, along with EU and EEA member states, until the rule was repealed by the appropriate competent national minister. At the same time, on the one hand, the 2018 Act made the British domestic data protection system more consistent. On the other, British and European business entities have had to comply with the requirements of two different legal systems since the end of the transition period. Thus, the extraterritorial scope of EU and UK legislation forces digital platforms applying to data subjects residing in different jurisdiction to apply to both regimes, which may no longer be in harmony with one another.[27]

Discussions

The Trade and Cooperation Agreement between the European Union and Great Britain signed on Christmas Eve of 2020 largely established the legal framework for the future architecture of relations between the parties in trade, the economy, and other areas (Babynina, 2021). The UK ratified this Agreement almost immediately by passing the European Union (Future Relations) Act of 2020. Within the EU, ratification stretched until April 29, 2021, when, after receiving the consent of the European Parliament on 27 April,[28] the Council of the EU decided on ratification. Until then, the previous EU legal regulation applied to the United Kingdom in its entirety, as if the UK was still a member state, during an additional transition period, the maximum duration of which could be six months (Article 782 of the Agreement). The purpose of this transition period appears to have been twofold: on the one hand, it prevented a sudden halt in data flows between the EU and the UK. On the other, it gave the European Commission sufficient time to decide on adequacy. Indeed, the Agreement explicitly provides that this transition period would end as soon as a decision on adequacy was made, or, failing that, after six months, whichever came first.

Title III of Part II of the Agreement governs digital trade, i.e., commerce carried out by "electronic means." This section focuses on cross-border data-sharing and its protection. Both parties made a formal commitment to ensure sufficient data-sharing, while avoiding the imposition of requirements regarding its location, as well as equipment and networks. Both parties committed to recognizing and protecting the right to data protection and privacy in order to increase the level of trust between market participants. The EU and UK are free to develop their own legal frameworks for data protection and sharing, while being obligated to ensure that general purpose data transfers in the digital marketplace are appropriate. Part III of the Agreement is devoted to cooperation between law enforcement and judicial authorities. Both parties are committed to protecting personal data, along with other fundamental rights. The provisions of the Agreement confirmed the need to ensure

[27] Manancourt, V. (2020, December 28). What the interim Brexit data flows deal means for Britain. *Politico*. https://www.politico.eu/article/what-the-interim-brexit-data-flows-deal-means-for-britain/

[28] European Parliament. (2021). *European Parliament legislative resolution on the draft Council decision on the conclusion, on behalf of the Union, of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, and of the Agreement between the European Union and the United Kingdom of Great Britain and Northern Ireland concerning security procedures for exchanging and protecting classified information (05022/2021 — C9-0086/2021 – 2020/0382(NLE))*. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0140_EN.html

compliance with data protection principles, such as the principle of security and storage restrictions, in relation to this data.

Thus, by establishing the possibility of making an adequacy decision in relation to the UK as a non-member country, the European Commission also indicated the nature of the future relationship between the parties from the position of the sphere of personal data protection. Great Britain, as a former member state of the Union, will not be granted any special status, particularly with respect to automatic mandatory bilateral recognition of the adequacy of the level of protection, as originally proposed by the UK during the negotiations. From the point of view of the legal regulation of the protection of personal data, this rule lays the foundation for a potential divergence between the legal systems of the EU and UK, which, in the context of the adopted bilateral documents, can develop independently, without being tied to a specific architecture for the chosen model of future relations (Entin & Galushko, 2021).

The European Commission issues decisions on adequacy unilaterally, at its discretion, subject to an assessment of the adequacy of the legal system of the non-member country, and is obliged to update the decision regularly thereafter. Thus, the decision on adequacy is not final or irrevocable and can be withdrawn at any time. This is confirmed by the practice of the Court of Justice of the European Union, which, in its decision in the Schrems I case, pointed out that adequacy decisions are evolving documents reflecting the current state of the foreign legal system in question. Through these mechanisms, the European Commission certifies that the non-member country provides adequate guarantees to justify the authorization for the transfer of personal data out of the EU. Thus, a positive assessment of the adequacy of a non-member country can suddenly change in the event of reforms or the emergence of new legal regulatory mechanisms that affect the system of protection of cross-border personal data. This possibility clearly shows to what extent the British legal system (although formally already independent) will still be, de facto, subject to a number of restrictions implicitly derived from EU law.

Moreover, adequacy decisions can be challenged in the Court of Justice, as Mr. Schrems successfully did in relation to an adequacy decision related, firstly, to the privacy regime of the US (Safe Harbor principles) and then to a decision related to the approval of another mechanism introduced between the EU and the USA (the EU-US Privacy Shield). In addition, adequacy decisions can be suspended, since, if competent national authorities of EU member states have doubts about the adequacy of the data protection regime of a non-member country, they can suspend cross-border data-sharing with it (Fabbrini et al., 2021).

On May 21, 2021, the European Parliament adopted a resolution on the adequate protection of personal data by the UK[29] calling on the European Commission to make an appropriate decision on adequacy in relation to the United Kingdom. At the same time, as mentioned earlier, the EU Parliament once again expressed concern about the actions of the UK in this area. Firstly, inappropriate law enforcement practices of the British authorities in relation to compliance with EU law was noted, particularly with respect to the EU's GDPR. In addition, there were problems in the immigration sphere, plus concerns about mass surveillance by British intelligence services and the subsequent transfer of personal data, primarily to American authorities and services. At the same time, the resolution welcomes the fact that the decision of the European Commission will only apply for four years, while calling on it to constantly monitor the relevant practices applied by the British authorities.

[29] European Parliament. (2021). *European Parliament resolution on the adequate protection of personal data by the United Kingdom (2021/2594(RSP))*. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0262_EN.htm

Finally, on June 28, 2021, the European Commission adopted an adequacy decision for the United Kingdom under the GDPR. Since that time, it has been possible to freely conduct data-sharing between the European Union and the United Kingdom, where it benefits from an essentially equivalent level of protection to that guaranteed under EU law. The adequacy decision also facilitated the correct implementation of the EU-UK Trade and Cooperation Agreement, as it includes strong safeguards in case of future divergence, such as a 'sunset clause' that limits the duration of adequacy to four years.[30]

Moreover, to build upon this, the UK Government has established a new post-Brexit council to ensure that personal data transfers around the world match the protection they have in Britain.[31] On January 25, 2022, a group of experts consisting of the world's leading academics and digital industry figures (including representatives of Google, Mastercard, and Microsoft) met for the first time to help Britain seize the opportunities of better global data sharing. The International Data Transfer Expert Council was launched to provide independent advice to the government so that it could achieve its mission to unlock the benefits of free and secure cross-border data flows now that the country has left the EU.[32] This is one of the measures enshrined in the UK government's recent consultative document, 'Data: A New Direction', which explores various ways in which the UK might reform its data protection regime, but does not actually state a change in policy.[33]

On July 18, 2022, the Data Protection and Digital Information Bill[34] was introduced in the British House of Commons, containing a package of amendments to the UK's data protection regime. The Bill is currently making its way through Parliament, but very slowly. This is due to the change to the UK's governmental leadership. The Bill's impact assessment states that «the government's view is that reform of UK legislation on personal data is compatible with the EU maintaining free flow of personal data from Europe».[35] However, whereas the proposed multiple amendments the Bill looks quite different to the EU' regulatory approach in the field. The more the UK diverges from GDPR, the more likely its adequacy agreement with the EU could be undermined.[36] Those seeking a substantial streamlining of requirements and the removal of obstacles to innovation and business may feel the Bill does not go far enough; on the other hand, the proposals could be viewed as diverging sufficiently from the EU GDPR to threaten the UK's adequacy status, which to be reviewed in 2024. Much depends on the balance struck in the final text of the Bill. In any case, the EU's rules compliance is a huge influencing factor in the UK's legal drafting even after Brexit.

Another recent example may be added here to support our thesis on the EU's influence on co-regulation. The European Commission has decided to allow personal data to be transferred from the

30 European Commission. (2021). *Data protection: Commission adopts adequacy decisions for the UK.* https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183

31 Phillips, A. (2022, January 25). Brexit truimph: UK forges ahead with tech giants to use new powers to boost data flow. *Express.* https://www.express.co.uk/news/uk/1555689/Brexit-news-Britain-tech-giants-data-flow-protection-privacy-google-microsoft

32 UK Government. (2022). *Global data experts fire up government's plans to promote free flow of data: Press release.* https://www.gov.uk/government/news/global-data-experts-fire-up-governments-plans-to-promote-free-flow-of-data

33 Dove, E. (2021, November 10). Data: A new direction — But which direction? A commentary on the UK Government's public consultation on reforms to the data protection regime. *The Mason Institute Blog.* https://blogs.ed.ac.uk/mason-institute/2021/11/10/data-a-new-direction-but-which-direction-a-commentary-on-the-uk-governments-public-consultation-on-reforms-to-the-data-protection-regime-by-edward-dove/

34 UK Parliament (2022). *Data Protection and Digital Information Bill.* https://bills.parliament.uk/bills/3322

35 UK Government. (2022). *Data Protection and Digital Information Bill: Impact assessments.* https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impact-assessments

36 *UK to reform data protection, throwing EU adequacy ruling into doubt.* https://www.euractiv.com/section/digital/news/uk-to-reform-data-protection-throwing-eu-adequacy-ruling-into-doubt/

European Union to South Korea under the GDPR.[37] The adequacy decision was issued only after amendments were added to South Korea's Personal Information Protection Act (PIPA), which strengthened the investigatory and enforcement powers of PIPC, South Korea's independent data protection authority. Furthermore, during the adequacy talks, the European Commission and the PIPC agreed on several additional safeguards to increase the protection of personal data processed in South Korea, including with respect to transparency (by requiring South Korean digital platforms to inform Europeans about the processing of their data) and onward data transfers (by ensuring that data continues to benefit from the same level of protection when further transferred to third-party countries).[38]

After the recognition by the European Court of Justice in 2020 of the EU-US Privacy Shield as a document that no longer ensures the proper and legal transfer of personal data from the territory of the European Union to the United States of America,[39] there were many misunderstandings when US companies operate in the EU territory.[40] And the United States and the European Commission have agreed in principle on a new Transatlantic Data Privacy Framework that will make it easier for companies to transfer personal data, including employee data, from the EU member-states to the United States.[41] The new framework cooperation, announced in March 2022, aims to address the privacy concerns referred to by the EU Court of justice in 2020 when it invalidated the previous EU-US Privacy Shield document.

The Transatlantic Data Privacy Framework aims to introduce better privacy protections to limit US intelligence activities related to the personal data of EU residents and allow EU residents to claim compensation through an independent Data Protection Court.

The European Commission cited several key principles of the new structure, noting that:

- based on the new framework, data will be able to flow freely and safely between the EU and participating U.S. companies;
- a new set of rules and binding safeguards to limit access to data by U.S. intelligence authorities to what is necessary and proportionate to protect national security;
- U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards;
- a new two-tier redress system to investigate and resolve complaints of Europeans on access of data by U.S. Intelligence authorities, which includes a Data Protection Review Court;
- strong obligations for companies processing data transferred from the EU, which will continue to include the requirement to self-certify their adherence to the Principles through the U.S. Department of Commerce;

---

37 European Commission. (2021). *Commission implementing Decision of 17.12.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act.* https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf

38 BlankRome. (2022, January). *The BR Privacy & Security Download.* https://www.blankrome.com/publications/br-privacy-security-download-january-2022

39 European Court of Justice (2020). *Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. Request for a preliminary ruling from the High Court (Ireland).* https://curia.europa.eu/juris/liste.jsf?num=C-311/18

40 Cory, N., Castro, D., & Dick, E. (2020, December 3) *'Schrems II': What invalidating the EU-US privacy shield means for transatlantic trade and innovation. Information Technology and Innovation Foundation.* https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic/

41 The White House (2022). *Fact sheet: United States and European Commission announce Trans-Atlantic Data Privacy Framework.* https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

- specific monitoring and review mechanisms.[42]

While many of the details still remain unclear, the US and European Commission have represented that the next steps will be to translate the agreement in principle into legal documents.[43] And the tendency will continue. According to the European Commission's Data Act, which was published on February 23, 2022, digital platforms like Amazon and Microsoft must set up safeguards against illegal data transfers to non-EU governments,[44] thus pushing the development of national legal arrangements in the sphere. The developments will be keenly followed by a number of tech giants like Meta, which is at risk of a suspension order being slapped on its EU-US data transfers following a long-running complaint that's still grinding through the EU's GDPR enforcement procedures.[45] Google, whose analytics product has been hit with warnings by DPAs around the bloc over illegal transfers of personal data, should be also added to the list.[46] In this regard should be also mentioned Microsoft, whose cloud-based productivity suite 365 is under GDPR review by German DPAs that's further complicated by the data transfers issue, to name three high profile examples.[47]

Conclusions

This study shows that the problem of personal data protection in contemporary conditions has the same origin and requires the same solution — to maintain an optimal balance between human rights, society, and the state. The means of establishing a balance of rights is a legal regime for the protection of personal data that is based on certain principles common to all democratic states, regardless of the specific features of their legal systems. This set of principles constitutes a body of good information practice: there should be no personal data processing systems in which the existence of personal data processing is secret: the person must be notified about the processing and use of their personal data, provided with the opportunity to know what information their personal data contains, be informed about why such data is cultivated, and how it is used. People should also be able to prevent the use or dissemination of their personal data for purposes they have not agreed upon and given the opportunity to make corrections or additions to their personal data. In addition, all organizations that process or use data in a form that allows identification of an individual should be required to take measures against the misuse of personal data, and personal data should only be used for the purposes for which it was collected.

With regard to the example of the UK's withdrawal from the European Union, it can be stated that the British legal regime still maintains a certain dependence on the EU and its legal order, since, as a non-member country, it does not have the ability to influence decisions made in the Union. In addition, in principle, Brexit has complicated the cross-border activities of digital platforms in

[42] European Commission (2022). *Trans-Atlantic Data Privacy Framework*. https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100

[43] TrustArc Privacy Intelligence (2022). *New EU-US Agreement: Trans-Atlantic Data Privacy Framework*. https://trustarc.com/blog/2022/03/25/trans-atlantic-data-privacy-framework/

[44] Chee, F. Y. (2022, February 4). EU aims to tighten curbs on data transfers to non-EU governments — EU document. *Reuters*. https://www.reuters.com/business/eu-aims-tighten-curbs-data-transfers-non-eu-governments-eu-document-2022-02-03/

[45] Lomas N. (2022, August, 11). Facebook avoids a service shutdown in Europe for now. *TechCrunch*. https://techcrunch.com/2022/08/11/facebook-europe-shut-down-delay/

[46] Lomas N. (2022, February, 10). France's privacy watchdog latest to find Google Analytics breaches GDPR. *TechCrunch*. https://techcrunch.com/2022/02/10/cnil-google-analytics-gdpr-breach/

[47] Lomas N. (2022, February, 15). Public sector bodies' use of cloud services probed in joint EU data protection enforcement. *TechCrunch*. https://techcrunch.com/2022/02/15/edpb-cef-public-sector-cloud/

both jurisdictions, since the uniform legal regulation within the EU for all member states has been replaced by a dichotomy in the form of the presence and interaction of the relevant legal norms of both the UK and the European Union, which must now be followed, and which may contain mutual contradictions.

In legally regulating data protection, the UK is forced to obey the EU's legal order and is dependent on the will and legal prescriptions of the Union's institutions, primarily with respect to the need to receive an adequacy decision from the European Commission. However, even after the adoption of such a decision, the legal order of the United Kingdom will still be under the EU's constant control with respect to the assessment of the level of adequacy of its system of personal data protection and ensuring sufficient data-sharing, which casts doubt on the stability and predictability of relations in this area, thus shifting the degree of influence in the co-regulation to the EU's supranational authorities. This is also confirmed by the examples of other third countries, in particular South Korea and the United States, demonstrating the importance of strengthening and developing European integration mechanisms that can successfully overcome the reverse of integration, not only minimizing the negative consequences of disintegration, but also strengthening international integration and additionally influencing the legal orders of states that are not part of the integration entity.

References

1. Babynina, L. O. (2021). Torgovoe soglashenie mezhdu ES i Velikobritaniej: Mezhdu kondicional'nost'ju i suverenitetom [Trade and cooperation agreement between the EU and the UK: Conditionality versus sovereignty]. *Sovremennaja Evropa*, (2), 5-16. http://dx.doi.org/10.15211/soveurope220210516
2. Beck, E. J., Gill, W., & De Lay, P. R. (2016). Protecting the confidentiality and security of personal health information in low- and middle-income countries in the era of SDGs and Big Data. *Global Health Action, 9*(1), 32089. https://doi.org/10.3402/gha.v9.32089
3. Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review,* 107(1), 19-35.
4. De Hert P., & Papakonstantinou, V. (2017). The rich UK contribution to the field of EU data protection: Let's not go for "third country" status after Brexit'. *Computer Law & Security Review, 33*(3), 354-360. https://doi.org/10.1016/j.clsr.2017.03.008
5. Eisenmann, T., Geoffrey, P., & Van Alstyne, M. (2011). Platform envelopment. *Strategic Management Journal, 32*(12), 1270-1285. https://doi.org/10.1002/smj.935
6. Entin, M., & Galushko, D. (2021). O pravovykh posledstviyakh Brekzita (na primere zashchity personal'nykh dannykh) [On the legal consequences of Brexit (on the example of personal data protection)]. *Sovremennaya Evropa, 105*(5), 45-55. http://dx.doi.org/10.15211/soveurope520214555
7. Fabbrini, F., Celeste, E., & Quinn, J. (Eds.) (2021). *Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty*. Hart Publishing.
8. Kira, B., Sinha, V., & Srinivasan, S. (2021). Regulating digital ecosystems: Bridging the gap between competition policy and data protection. *Industrial and Corporate Change, 30*(5), 1337-1360. https://doi.org/10.1093/icc/dtab053
9. Martirosjan, A. Z. (2021). Realii cifrovogo suvereniteta v sovremennom mire [Realities of Digital Sovereignty in the Modern World]. *Mezhdunarodnaja Zhizn*, (3), 28-35. https://interaffairs.ru/jauthor/material/2483
10. Mingers, J., & Standing, C. (2018). What is information? Toward a theory of information as objective and veridical. *Journal of Information Technology, 33*(2), 85-104. https://doi.org/10.1057/s41265-017-0038-6
11. Nicolaïdis, K. (2017). The political mantra: Brexit, control and the transformation of the European order. In F. Fabbrini (Ed.), *The Law & Politics of Brexit.* Oxford University Press.

12. Nitecki, J. Z. (1985). The concept of information-knowledge continuum: Implications for librarianship. *The Journal of Library History (1974-1987), 20*(4), 387-407. http://www.jstor.org/stable/25541654
13. Prosser, W. L. (1964). *Handbook of the Law of Torts*. West Publication Corp.
14. Resta, G. (2011). The new frontiers of personality rights and the problem of commodification: European and comparative perspectives. *Tulane European and Civil Law Forum, 33*, 49-57.
15. Voigt, P. & von dem Bussche, A. (2017). *The EU general data protection regulation (GDPR). A practical guide*. Springer.
16. Voss, W.G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. *Journal of Law, Technology & Policy, 2*, 405–463.
17. Voss, W.G. (2020). Cross-Border data flows, the GDPR, and data governance. *Washington International Law Journal*, 29(3), 485-532.
18. Walker, R. (2015). *Success with big data: From data and analytics to profits.* Oxford University Press.

Information about the authors:

Mark L. Entin — Dr. Sci. in Law, Professor, Head of European Law Department, MGIMO-University, Moscow, Russia.
entinmark@gmail.com
ORCID: https://orcid.org/0000-0001-9562-8340

Ekaterina G. Entina — Dr. Sci. in Politics, Associate Professor, Director of Mediterranean Studies Centre, Faculty of World Economy and International Affairs, HSE University, Moscow, Russia.
e.entina@hse.ru
ORCID: https://orcid.org/0000-0003-4198-4870

Dmitriy V. Galushko — PhD in Law, Associate Professor, Department of Legal Regulation of Economic Activity, Financial University, Moscow, Russia.
galushkodv@gmail.com
ORCID: https://orcid.org/0000-0001-9562-8340

Сведения об авторах:

Энтин М. Л. — доктор юридических наук, профессор, заведующий кафедрой европейского права Московского государственного института международных отношений (МГИМО-Университет) МИД России, Москва, Россия.
entinmark@gmail.com
ORCID: https://orcid.org/0000-0001-9562-8340

Энтина Е. Г. — доктор политических наук, доцент, директор центра средиземноморских исследований Факультета мировой экономики и мировой политики Национального исследовательского университета «Высшая школа экономики», Москва, Россия.
entinmark@gmail.com
ORCID: https://orcid.org/0000-0003-4198-4870

Галушко Д. В. — кандидат юридических наук, доцент, доцент департамента правового регулирования экономической деятельности Финансового университета при Правительстве Российской Федерации, Москва, Россия.
galushkodv@gmail.com
ORCID: https://orcid.org/0000-0002-4484-9423

https://doi.org/10.38044/2686-9136-2022-3-4-89-106

СТАТЬИ

ПРАВО НА ЗАБВЕНИЕ: НОВОЕ ПРАВО ЧЕЛОВЕКА?

Е.С. Чуб

ОАО «Автомир»
350004, Россия, Краснодар, ул. Кропоткина, 50

Аннотация

В статье рассматривается вопрос необходимости закрепления «права на забвение» как нового права человека в контексте соотношения с правом на неприкосновенность частной жизни. Его законодательное развитие и глобальное применение ставят под вопрос соотношение между частными и публичными интересами. Речь идёт, с одной стороны, о защите частной жизни отдельного лица, с другой — о свободе информации и выражения мнений. В связи с этим цель исследования заключается в определении подхода для закрепления «права на забвение» таким образом, чтобы при этом был обеспечен оптимальный баланс интересов.

Исследуя эволюцию признания «права на забвение», проблемы его применения, а также влияние на свободный доступ к информации и свободу выражения мнений, автор статьи рассматривает текущее состояние данного института. Так как «право на забвение» изначально возникло в Европейском союзе, в статье исследуется законодательство и правоприменительная практика «права на забвение» в Российской Федерации и Европейском союзе, по итогам чего делается вывод о необходимости понимания «права на забвение» как самостоятельной категории и необходимости совершенствования действующего российского законодательства. В частности, предлагается дополнить п. 1 ст. 10.3 ФЗ «Об информации, информационных технологиях и защите информации» положением о том, что оператор поисковой системы вправе отказать в удовлетворении заявления об удалении ссылок в тех случаях, когда информация, содержащаяся в них, имеет общественную значимость или представляет общественный интерес.

Ключевые слова

право на забвение, защита частной жизни, Европейская конвенция по правам человека, персональные данные, права человека, Европейский союз

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Чуб, Е. С. (2022). Право на забвение: новое право человека? *Цифровое право, 3*(4), 89–106. https://doi.org/10.38044/2686-9136-2022-3-4-89-106

Поступила: 23.07.2022, принята в печать: 23.08.2022, опубликована: 31.12.2022

ARTICLES

THE RIGHT TO BE FORGOTTEN: A NEW HUMAN RIGHT?

Elena S. Chub

OAO Avtomir
50, Kropotkina str., Krasnodar, Russia, 350004

Abstract

The article analyzes the need to establish the "right to be forgotten" as a new human right in the context of the correlation with the right to privacy. Its legislative development and global application call into question the relationship between private and public interests. The issue includes protection of an individual's privacy, on the one hand, and freedom of information and expression on the other. In this context, the purpose of the study is to identify an approach to enshrine the "right to be forgotten" in a way that strikes an optimal balance of interests.

Exploring the evolution of the "right to be forgotten" and the problems of its enforcement, as well as its impact on free access to information and freedom of expression, the author examines the current state of this institution. As the "right to be forgotten" originally appeared in the European Union, the article examines legislation and law enforcement practice of the "right to be forgotten" in the Russian Federation and the European Union, which leads to the conclusion that the "right to be forgotten" should be considered as an independent category in the current Russian legislation. It is proposed to supplement item 1 clause 10.3 of Federal Law "On Information, Information Technology and Information Security" with a provision that the operator of a search engine has the right to refuse to satisfy requests to remove references in cases where the information is of public interest.

Keywords

right to be forgotten, data protection and privacy, European Convention on Human Rights, personal data, human rights, European Union

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Chub, E. S. (2022). The right to be forgotten: A new human right? *Digital Law Journal*, *3*(4), 89–106. https://doi.org/10.38044/2686-9136-2022-3-4-89-106

Submitted: 23 July 2022, accepted: 23 Aug. 2022, published: 31 Dec. 2022

Введение

В эпоху цифровых технологий информация в Интернете стала широко распространенной и постоянно доступной. Поисковые системы представляют собой необходимый инструмент, которым современный человек пользуется практически каждый день для поиска сведений. Европейский суд по правам человека признал Интернет одним из основных средств, с помощью которых люди реализуют право на свободу выражения мнения и другие права, связанные с информацией[1]. В контексте Интернета, информационных технологий и социальных сетей, активно оказывающих влияние на все сферы общества, включая право, следует отметить, что благодаря развитию Сети появляются новые информационные права, среди которых и «право на забвение».

«Право на забвение» как идея, не имеющая практического воплощения, возникло еще в XX в. в связи с повсеместным распространением Интернета. Первой значимой вехой в его регулировании стало принятие Директивы № 95/46/ЕС Европейского парламента и Совета ЕС от 24 октября 1995 г. о защите данных (далее — Директива № 95/46/ЕС), в которой впервые были заложены основы для дальнейшего закрепления «права на забвение» в ЕС.

В России указанное право было закреплено относительно недавно (с 1 января 2016 г.) путем внесения поправок в законодательство об информации. В Федеральном законе от 13 июля 2015 г. № 264-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации» заинтересованным лицам было предоставлено право требовать от операторов поисковых сетей прекращения распространения информации, которая соответствует описанным в законе критериям. Тем не менее указанный акт был подвергнут серьезной критике в связи с тем, что он (1) не гарантировал удаления сведений с источника информации; (2) не установил четких критериев информации, к которой может применяться «право на забвение»; (3) не определил соотношение «права на забвение» с иными конституционно закрепленными правами, такими как право на свободу выражения мнения или право на доступ к информации. Ввиду указанных проблем возникает необходимость совершенствования российского законодательства по данному вопросу на основании анализа зарубежного опыта и судебной практики.

Целями исследования являются изучение возможности рассматривать «право на забвение» как новый вид права и анализ его соотношения с правами человека предыдущих поколений (правом на выражение мнения и правом на доступ к информации) для внесения соответствующих изменений в российское законодательство.

Гипотеза исследования заключается в том, что «право на забвение» представляет собой самостоятельное право, которое нуждается в отдельном закреплении на законодательном уровне для отграничения его от других информационных прав.

Генезис и толкование «права на забвение»

«Право на забвение» (англ. *right to be forgotten*) — концепция, применявшаяся в судебной практике Европейского союза, а также в Аргентине в конце XX в. Так, согласно «праву на забвение» пользователь имеет право запросить удаление в поисковых системах и других каталогах сети Интернет определенной информации, которая может нанести вред его чести и достоинству. «Право на забвение» фактически применяется либо путем удаления сведений с исходного

[1] Cengizand Others v. Turkey, 2015-VIII Eur. Ct. H.R. http://hudoc.echr.coe.int/eng?i=001-159188

сайта («право на стирание» *(right to erasure)*), либо путем разыменования веб-сайта поисковыми системами («право на разыменование» *(right to dereferencing)*) (Maietta, 2020).

Начиная с 1970-х гг., в условиях развития цифровых технологий, концепция защиты конфиденциальности все больше пересекается с идеей защиты персональных данных. «Право на забвение» рассматривается как реакция на цифровые технологии, в противовес свободе информации, и как ключевой компонент защиты новых форм конфиденциальности. Фактически «право на забвение» является одним из основных прав человека XXI в., и его признание будет только расширяться, несмотря на множество аргументов против его применения.

Сторонники «права на забвение» считают его справедливым инструментом, который позволяет избежать негативного влияния компрометирующей информации на жизнь человека. Его критики утверждают, что существует риск того, что люди получат возможность переписать свое прошлое или даже полностью стереть негативные моменты своей биографии. Кроме того, противники «права на забвение» связывают его с угрозой для свободы выражения мнения и свободного доступа к информации. Право человека решать, что другие могут «помнить» о нем, не только бросает вызов существующим принципам свободы выражения мнений, но и противоречит практике обмена информацией в Интернете (Cofone, 2020).

«Право на забвение» также может отрицательно сказаться на обработке данных, необходимых для целей статистики, научных и исторических исследований. Таким образом, «право на забвение» может создать угрозу архивной работе специалистов, что приведет к исчезновению информации, необходимой для понимания и анализа определенных исторических событий (Jones, 2016).

В теоретическом смысле «право на забвение» рассматривается как право лиц самостоятельно определять, когда, как и в какой степени информация, касающаяся их, передается другим лицам, или как право человека осуществлять контроль над сведениями, которые напрямую относятся к его личности. «Право быть забытым» вытекает из действия права на неприкосновенность частной жизни, несмотря на то что оно применяется к информации, в определенной степени ставшей общественным достоянием.

«Право на забвение» не закреплено в международных договорах о правах человека и национальных конституциях. Сфера его применения остается в значительной степени неопределенной: она может варьироваться от ограниченного права, подпадающего под действие законодательства о защите персональных данных, до более широких концепций, включающих защиту репутации, чести и человеческого достоинства.

Исторически концепция «права на забвение» возникла из идеи о том, что при приеме на работу не следует учитывать прошлое кандидата. С появлением Интернета и поисковых систем записи о прошлом людей стали доступны в свободной форме. Начиная с Директивы № 95/46/ЕС, физическим лицам было предоставлено право удалять все связанные с ними персональные данные, когда они покидают службу или закрывают учетную запись. «Право на забвение» впервые было закреплено в законодательстве Французской Республики *(droit à l'oubli)*. В 2010 г. Франция приняла Хартию о праве на забвение, которая регулировала правовые отношения Французской Республики с частными компаниями в сфере защиты персональных данных граждан.

Толкование «права на забвение» было расширено в 2014 г. после знаменательного решения Суда ЕС *(The Court of Justice of the European Union (CJUE))* по делу *Google Spain,* в котором впервые было признано, что принципы защиты персональных данных применимы к публикации результатов поисковых систем. Так, в 2010 г. Марио Гонзалес подал жалобу в Национальное агентство защиты персональных данных Испании *(Agencia Española de Protección de Datos (AEPD))*

на международную поисковую систему *Google* по причине того, что в поисковой выдаче *Google* индексировались ссылки на персональные данные Марио, а именно на информацию о его имущественном положении. Изначально Национальное агентство защиты персональных данных отклонило данное заявление. Однако позднее оно было передано в Верховный суд Испании, который запросил у Суда ЕС предварительные ответы на следующие вопросы.

Во-первых, применяются ли в таком случае механизмы защиты персональных данных, регламентируемые Директивой № 95/46/ЕС, регулировавшей защиту персональных данных до принятия Общего регламента о защите персональных данных *(General Data Protection Regulation (GDPR))* 2016 г.; во-вторых, распространяются ли положения Директивы № 95/46/ЕС по контролю за распространением персональных данных на поисковые системы, и, наконец, имеет ли субъект, чьи права были нарушены, право требовать удаления поисковых ссылок в индексации поисковых систем?

На первые два вопроса Суд ЕС дал положительный ответ. В отношении третьего вопроса Суд заявил, что данное положение противоречит праву на доступ к информации и поэтому не может соотноситься с положениями Директивы.

На основании данного дела Судом ЕС был создан прецедент, сформулировавший процедуру, в рамках которой любое заинтересованное лицо, если его права были нарушены, имеет право заполнить специальную форму в поисковой системе *Google*. Это позволяет удалить из индексации ссылки, порочащие честь и достоинство лица или раскрывающие его персональные данные. Однако следует отметить, что исходная информация не удаляется, так как «право на забвение» распространяется на удаление ссылки в *Google*, но не на устранение самих персональных данных с источника первичной публикации[2]. Проблема заключается в том, что для удаления сведений с самого сайта субъекту данных необходимо изучать каждую интернет-страницу, на которой размещена информация, и требовать от администраторов сайтов удаления или изменения контента.

Суд ЕС постановил, что каждый человек имеет право запросить разыменование его личных данных операторами поисковых систем, действующими в Европейском союзе. В то время как национальные суды, регулирующие органы по защите данных, операторы поисковых систем и эксперты по защите частной информации предпринимали попытки оценить последствия признания «права на забвение», несколько государств последовали примеру и приняли закон, посвященный «праву на забвение». Следовательно, «право на забвение» перестало быть исключительно европейской идеей и приобрело более широкое распространение, в том числе и в российском законодательстве.

«Право на забвение» в законодательстве Европейского союза

Впоследствии «право на забвение» было имплементировано в Общий регламент 2016 г. о защите персональных данных, но с двумя оговорками. Во-первых, удаление нежелательных ссылок осуществляется операторами поисковой системы после заполнения специальной формы поисковой системы, на которой индексируются нежелательные ссылки. При этом соответствующего решения суда не требуется. Во-вторых, удаляются не сами материалы, а только ссылки на них. Таким образом, нарушенные права восстанавливаются лишь частично, что не является в полной мере эффективным. Следовательно, «право на забвение» было определено не как полное удаление персональных данных, а как ограничение доступа к ним.

[2] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, Mario González, 2014 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

В деле *Google Spain* Суд ЕС также признал необходимость проведения теста для определения баланса между частными и публичными интересами. В решении было отмечено, что «право на забвение» не является абсолютным и может быть реализовано в тех случаях, когда право на защиту частной жизни превалирует над интересами общества в доступе к информации.

В решении 2003 г. по делу *Bodil Lindqvist*[3] Суд ЕС указал на то, что меры, принимаемые государствами-членами для обеспечения защиты персональных данных, должны соответствовать как положениям Директивы № 95/46/ЕС[4], так и цели поддержания баланса между свободой доступа к информации и защитой конфиденциальности. При этом, как было отмечено, ничто не препятствует тому, чтобы государство-член расширило сферу действия национального законодательства, включающего положения Директивы № 95/46/ЕС, на области, не входящие в сферу ее применения, при условии, что никакие другие положения законодательства сообщества не препятствуют этому.

Международная поисковая система *Google* получила с 2016 г. уже более миллиона запросов об удалении информации из индексационной системы, среди которых были удовлетворены лишь около 100[5]. А по состоянию на февраль 2018 г. поисковая система за четыре года получила более 2,4 млн запросов на удаление *URL*-адресов из поисковых запросов.

Территориальная сфера применения «права на забвения» также рассматривалась с позиции *CJEU*. Так, в сентябре 2019 г. Суд ЕС опубликовал решение по делу *Google v. CNIL*[6], в котором было установлено ограничение на глобальное применение «права на забвение».

Решением от 21 мая 2015 г. президент французского органа по защите данных — Национальной комиссии по информатике и свободам *(Commission nationale de l'informatique et des libertés (CNIL))* — направил официальное уведомление компании *Google* о том, что при удовлетворении запроса физического лица об удалении ссылок из результатов поиска, проведенного на основе его имени, она должна совершить это по всем доменным именам своей поисковой системы, т.е. во всем мире.

Компания *Google* отказалась выполнить это требование и удалила ссылки только из результатов поиска доменных имен государств — членов Европейского союза. Кроме того, *Google* отметил, что такая практика нарушает принципы вежливости и невмешательства, признанные международным публичным правом, и нарушает свободу выражения мнений, информации, коммуникаций и прессы, гарантированных, в частности, ст. 11 Хартии основных прав Европейского союза[7].

Суду необходимо было решить вопрос о территориальной сфере действия «права быть забытым»: следует ли толковать «право на забвение» как обязанность оператора поисковой системы удаления ссылок по всему миру, в пределах Союза или только на национальном уровне?

В решении по делу C-507/17 Суд ЕС постановил, что в соответствии с законодательством Европейского союза *Google* и другие операторы поисковых систем не обязаны применять европейское «право на забвение» во всем мире. В решении разъясняется, что хотя жители ЕС имеют

---

[3] Case C-101/01, Criminal proceedings against Bodil Lindqvist, 2013 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101

[4] Директива, действовавшая до принятия Общего регламента по защите данных, которая была отменена последним.

[5] Яндекс. (2016, 25 марта). *О применении закона «о праве на забвение»*. https://yandex.ru/blog/company/o-primenenii-zakona-o-prave-na-zabvenie

[6] Case C-507/17, Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), 2019 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CC0507

[7] Charter of Fundamental Rights of European Union, 2021 O.J. (C 326) 2. https://eur-lex.europa.eu/homepage.html

законное «право быть забытыми», оно применяется только в пределах границ государств — членов ЕС. Как пояснил Суд, несмотря на то что нормы *GDPR* могут применяться за пределами государств-членов, операторы при этом не обязаны удалять ссылки из поисковых систем стран, не входящих в Европейский союз.

В данном случае Суд установил ограничение территориального действия права физического лица на удаление персональных данных. Иначе говоря, *Google* должен удалять ссылки на персональные данные физического лица из поисковых запросов в Интернете, осуществляемых в рамках ЕС. Кроме того, Суд ЕС напомнил об экстерриториальном действии Общего регламента в соответствии со ст. 3 *GDPR*.

Хотя Суд признал ограничение «права на удаление», он также указал на важные моменты, которые предоставляют право судебным органам и органам по защите данных в ЕС требовать от операторов поисковых систем исключения ссылок из поисковых систем по всему миру. Так, Суд постановил, что государства-члены и органы по защите данных компетентны по своему усмотрению сбалансировать право на неприкосновенность частной жизни и защиту персональных данных с правом на свободу информации. Также Суд отметил, что государства — члены ЕС имеют право отступать от ограничений в отношении обработки персональных данных в оправданных случаях, а также в целях журналистики[8].

Одним из наиболее важных элементов в аргументации Суда являлось положение о том, что *Google* — это коммерческая компания, целью которой является обеспечение как можно большего доступа к информации в поисковой системе. При этом *Google,* будучи частной компанией, самостоятельно принимает конечное решение о квалификации информации, подпадающей под категорию «общественные интересы».

Данное дело добавило правовую определенность в отношении территориальной сферы действия «права на удаление». Однако это является лишь развитием судебной практики по защите данных в соответствии с *GDPR.* Несмотря на то что решение Суда внесло ясность в сферу территориального действия «права на забвение», по-прежнему отсутствуют четкие указания о том, как следует оценивать критерий сбалансированности между конфликтующими правами.

Фактически Суд ЕС возложил на частные компании ответственность за соблюдение прав человека, наделив их полномочиями судей и не предоставив при этом рекомендаций по реализации «права на забвение» в спорных ситуациях. Принимая во внимание новую роль поисковых систем в урегулировании баланса частных и публичных интересов, можно констатировать, что они вырастают из технологичных компаний в структуры управления персональными данными.

Впрочем, существует иное представление о территориальном действии «права на забвение». Так, согласно французской Национальной комиссии по информатике и свободам, отказ *Google* разыменовать ссылки на все расширения доменного имени поисковой системы представляет собой нарушение прав на удаление при условии, что ссылки остаются «доступными для любого пользователя, выполняющего поиск по другим расширениям поисковой системы»[9]. Так как современное цифровое общество выходит за рамки национальных границ, право на защиту данных может быть нарушено в случае, если поисковая система показывает результат в стране, не являющейся местом проживания субъекта данных. Из этого следует, что единые

[8] Case C-507/17, Google Inc. v. Nationale de l'Informatique et des Libertés (CNIL), 2019 http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:62017CJ0507')

[9] Décision 2015-047 du 21 mai 2015 mettant en demeure la société X. [Decision No. 2015-047 of May 21, 2015 giving formal notice to company X.] https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000030746525/

стандарты защиты данных должны иметь экстерриториальные последствия за пределами ЕС (Fabbrini et al., 2021). Со своей стороны, *Google* считает, что полномочия *CNIL* ограничены Францией и что Франция не может обоснованно принимать решения о расширениях в других странах, утверждая, что глобальное разыменование будет чрезмерным и ограничит свободу выражения мнений.

«Право на забвение» в законодательстве Российской Федерации

В Российской Федерации нормы, регулирующие «право на забвение», появились в 2016 г. Так, 1 января 2016 г. вступил в силу Федеральный закон от 13 июля 2015 г. № 264-ФЗ, согласно которому в законодательстве было закреплено «право быть забытым». Согласно этому нормативному правовому акту, российские пользователи Интернета имеют право скрывать недостоверную или устаревшую информацию о себе, независимо от того, наносят ли такие сведения ущерб их чести и достоинству.

Следует отметить, что, в отличие от *GDPR,* российский Закон о защите персональных данных не имеет экстерриториального действия. По общему правилу действие Закона не распространяется на нерезидентов, которые осуществляют сбор персональных данных граждан Российской Федерации за пределами Российского государства. Отечественная поисковая система «Яндекс» уже в первый год после вступления в силу норм о «праве на забвение» получила более 4000 обращений по вопросу удаления нежелательных ссылок, но из них были удовлетворены только 30%[10]. Одним из первых известных заявителей, прибегнувших к «праву на забвение», стал предприниматель Сергей Анатольевич Михайлов. Часть результатов поиска о нем была скрыта. Однако неизвестно, какие именно ссылки были удалены, так как поисковые системы не вправе раскрывать данные о применении «права быть забытым». Согласно ст. 10.3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации) оператор поисковой системы обязан сохранять в тайне информацию о факте обращения к нему заявителя с таким требованием[11].

Впрочем, здесь возникает другая проблема, которая заключается в том, что применение «права на забвение» в российской практике противоречит праву на свободный доступ к информации (ч. 4 ст. 29 Конституции РФ)[12]. До сих пор остается неизвестным, на каком основании или исходя из каких доказательств сведения о заявителе были удалены, поскольку информация об истце или объекте запроса не может быть раскрыта. Так, Конституционный Суд РФ в Постановлении от 25 мая 2021 г. № 22-П по делу о проверке конституционности п. 8 ч. 1 ст. 6 Федерального закона «О персональных данных» в связи с жалобой ООО «МедРейтинг» установил баланс между правом на защиту частной жизни и свободой распространения информации.

Данное Постановление было вынесено в связи с судебным разбирательством по вопросу удаления отзыва о медицинском работнике, размещенного на сайте СМИ «МедРейтинг». Общество «МедРейтинг» сослалось на то, что ст. 6 Федерального закона «О персональных данных», а именно положение о том, что «обработка персональных данных допускается в случаях, когда она необходима для осуществления профессиональной деятельности журналиста или законной деятельности СМИ при условии, что при этом не нарушаются права и законные

[10] Котова, Ю. (2021, 29 марта). *«Яндекс» раскрыл число запросов на удаление ссылок по закону о забвении.* Forbes. https://www.forbes.ru/newsroom/tehnologii/424805-yandeks-raskryl-chislo-zaprosov-na-udalenie-ssylok-po-zakonu-o-zabvenii

[11] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Собрание законодательства Российской Федерации 2006, № 31, ст. 3448.

[12] Конституция Российской Федерации. Российская газета, 25.12.1993, № 237.

интересы субъекта персональных данных», противоречит Конституции РФ. По мнению заявителя, отсутствие критериев разграничения баланса частных и публичных интересов препятствует осуществлению свободной журналистской деятельности СМИ.

По мнению Конституционного Суда РФ, сведения о медицинских работниках в силу законодательства подлежат опубликованию на интернет-порталах (ст. 79 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации») и поэтому являются общедоступными. Как следствие, не требуется согласие для обработки персональных данных медицинских работников. При этом Суд указал на то, что сведения о медицинских работниках представляют общественный интерес в силу специфики профессии и признания здоровья высшей ценностью. Такая оценка качества оказания медицинских услуг, как отзыв на интернет-портале, выступает одной из форм общедоступной информации.

Таким образом, распространение сведений о персональных данных медицинского работника не нарушает его прав и свобод. Однако Конституционный Суд РФ указал на то, что редакция СМИ обязана проводить предварительный контроль содержания подобных отзывов во избежание суждений, содержащих оскорбления и иные высказывания, запрещенные нормами публичного права (ст. 5.61 КоАП РФ)[13]. При неоднократном нарушении издательством СМИ порядка размещения персональных данных медицинского работника, например сведений, заведомо порочащих честь и деловую репутацию (ст. 152 ГК РФ), а также сведений, содержащих признаки клеветы (ст. 128.1 УК РФ), медицинский работник имеет право воспрепятствовать размещению его персональных данных и отзывов о его профессиональной деятельности[14].

Необходимо отметить, что вышеописанный случай из правоприменительной практики относится к специальному законодательству и ст. 10.3 Закона об информации среди исключительных случаев отказа в применении «права на забвение» не упоминает такой фактор, как «общественная значимость» сведений.

Актуальные проблемы «права на забвение»

Для определения других проблем при реализации в нашей стране «права на забвение» целесообразно обратиться к европейскому законодательству, учитывая, что в пояснительной записке к Проекту федерального закона «Об информации, информационных технологиях и о защите информации» указывается на стремление законодателя продолжить политику противодействия дезинформации в Интернете, начатую Европейской комиссией[15].

Статья 10.3 Закона об информации устанавливает перечень сведений, которые могут быть удалены оператором поисковой системы по требованию заявителя: (1) информация, распространяющаяся с нарушением действующего законодательства; (2) являющаяся недостоверной; (3) потерявшая актуальность; (4) уже утратившая значение для заявителя по причине его дальнейших действий. Тем не менее оператор не обязан прекращать выдачу, если информация содержит сведения о событиях, содержащих признаки уголовно наказуемых деяний, сроки

[13] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 01.07.2021), Собрание законодательства Российской Федерации 2002, № 1, ст. 1.

[14] Постановление Конституционного суда Российской Федерации от 25 мая 2021 г.№ 22-П «По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона «О персональных данных» в связи с жалобой общества с ограниченной ответственностью «МедРейтинг». Российская газета от 08 июня 2021 г.

[15] Проект федерального закона «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” (в части применения информационных технологий в целях идентификации граждан Российской Федерации)» (№ 946734-7). https://sozd.duma.gov.ru/bill/946734-7

привлечения к уголовной ответственности по которым не истекли, и сведения о совершении гражданином преступления, по которому не снята или не погашена судимость.

Практика применения норм о «праве гражданина на забвение» показывает, что в России «право на забвение» в некоторых случаях конфликтует с правом на доступ к информации, а также ограничивает последнее, что в корне не согласуется с ч. 4 ст. 29 Конституции РФ.

Право на свободу выражения мнений и свободный доступ к информации распространяется на все СМИ и является неотъемлемой частью свободы личности. Право на свободу выражения мнений признается практически во всех национальных конституциях и в большинстве международных договоров по правам человека, включая Всеобщую декларацию прав человека, Международный пакт о гражданских и политических правах (далее — МПГПП).

Тем не менее свобода выражения мнений не является правом абсолютным. Международные договоры по правам человека ограничивают данное право определенными условиями реализации. Так, согласно ст. 19 МПГПП ограничения возможны в случаях, когда: (1) такое ограничение законодательно предусмотрено; (2) существуют законные цели ограничения, прямо изложенные в данной статье; (3) такие ограничения представляются необходимыми в демократическом обществе[16]. В частности, требование необходимости подразумевает, что принятая мера пропорциональна желаемой цели. Если менее обременительная мера способна достичь той же цели, следует применять наименее ограничительную меру.

Таким образом, международное право допускает определенные ограничения свободы выражения мнений с целью защиты других законных интересов, включая права третьих лиц.

Баланс между правом на свободу выражения мнений и правом на уважение частной жизни на практике вызывает споры. С одной стороны, защита права на неприкосновенность частной жизни в Интернете имеет решающее значение для того, чтобы пользователи имели возможность свободного осуществления права на свободу выражения мнений (например, путем сохранения анонимности). С другой — публикация информации частного характера является грубым нарушением права на неприкосновенность частной жизни (Mendel, 2018). В то же время оба этих права могут быть ограничены при условии соответствия тройному тесту. Это означает, что государства не обязаны принимать меры по защите частной жизни, если это является чрезмерным ограничением свободы выражения мнений[17]. Одновременно в соответствии с международным правом в области прав человека государства обязаны предоставлять средства правовой защиты в случае нарушений обоих прав. Другими словами, свобода выражения мнений и право на неприкосновенность частной жизни дополняют друг друга, но иногда вступают в конфликт. Эти конфликты особо трудно разрешить в тех случаях, когда соответствующая информация является одновременно как личной, так и публичной.

Одним из принципиальных отличий регулирования «права на забвение» в Европейском союзе является его закрепление в специальном законодательстве о защите персональных данных. Речь идет о *GDPR*. В российском законодательстве «право на забвение» не имеет самостоятельного закрепления в отдельном акте, поскольку включается в Закон об информации. Некоторая связь с категорией персональных данных обеспечивается за счет уже упомянутого Постановления Конституционного Суда РФ от 25 мая 2021 г. № 22-П.

В соответствии с положениями ст. 17 *GDPR* «право на забвение» применяется в ряде случаев.

---

[16] International Covenant on Civil and Political Rights art 19, Dec. 19, 1966, 999 U.N.T.S. 178. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[17] Mosley v. United Kingdom, 2011 Eur. Ct. H.R. https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-3532678-3987591&filename=Arret%20de%20chambre%20Mosley%20c.%20Royuame%20Uni%2010.05.11.pdf

Во-первых, когда удаляемые персональные данные больше не соответствуют целям, для которых они были первоначально собраны, или когда они были обработаны иным образом, например, если был расторгнут договор, содержащий персональные данные лиц.

Во-вторых, когда заинтересованное лицо отзывает свое согласие на обработку персональных данных.

В-третьих, с того момента, когда нет никаких юридических оснований для их обработки. Как правило, речь идет о конфиденциальных данных.

В-четвертых, когда данные были собраны в рамках услуги, предлагаемой несовершеннолетним, т.е. когда соответствующее лицо было еще несовершеннолетним на момент сбора данных.

Наконец, при наличии юридического обязательства удалять данные и когда заинтересованное лицо выступает против обработки своих данных, а орган, отвечающий за обработку данных, не имеет оснований, побуждающих его оставить без удовлетворения запрос об удалении.

Общий регламент о защите персональных данных предусматривает детальный перечень оснований удаления сведений, содержащих персональные данные заявителя. В соответствии со ст. 17 *GDPR* оператор обязан удалить сведения в случаях: (1) если они больше не нужны для целей, для которых они были собраны или обработаны; (2) заинтересованное лицо отзывает согласие, на котором основана обработка персональных данных, если отсутствует иное законное основание для обработки персональных данных; (3) персональные данные были подвергнуты незаконной обработке; (4) заинтересованное лицо выступает против обработки персональных данных, при этом отсутствуют законные основания для обработки данных; (5) персональные данные собирались в ходе предоставления услуг информационного общества[18].

Среди исключений, к которым не применяется «право на забвение», *GDPR* приводит: (1) случаи, когда обработка необходима для реализации права на свободу выражения мнения и свободный доступ к информации; (2) с целью выполнения юридических обязательств, предусмотренных законодательством Европейского союза или законодательством государства-члена, которому подчиняется оператор персональных данных; (3) с точки зрения общественного интереса в сфере здравоохранения; (4) в архивных целях, в общественных интересах, в целях научных или исторических исследований или в статистических целях; (5) в рамках правовых требований и исков. Так, в 2014 г. Апелляционный суд Парижа рассмотрел дело, в котором лицо, осужденное несколькими годами ранее, заявило о прекращении распространения документального фильма, повествующего о причинах его осуждения. В своем решении Суд отметил, что в данном случае «право на забвение» не превалирует над правом общественности «на исчерпывающую и объективную информацию». Кроме того, он также констатировал, что «связь с уже раскрытыми публичными фактами сама по себе не может представлять собой посягательство на неприкосновенность частной жизни»[19].

---

[18] Le Règlement général sur la protection des données personnelles (RGPD) 2018 Ordonnance 2018-1125 du 12 décembre 2018 relative à la protection des données personnelles et portant modification de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel [The General Regulations on the Protection of Personal Data (RGPD) 2018 Ordinance 2018-1125 of December 12, 2018 relating to the protection of personal data and amending Law 78-17 of January 6, 1978 relating to data processing, files and freedoms and various provisions concerning the protection of personal data], https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037800506

[19] Courd'appel de Paris, pôle 2, chambre 7, Feb. 26, 2014, No. RG 13/01241 https://www.doctrine.fr/d/CA/Paris/2014/R6194A8E202763C55CC93

Еще в знаковом решении по делу *Google Spain* Суд ЕС указал на то, что «право на забвение» не следует применять в тех случаях, когда имеются особые причины, такие как роль, которую играет указанное лицо в общественной жизни. Если станет очевидным, что вмешательство в его основные права оправдано тем, что общественность заинтересована в том, чтобы в результате такого включения иметь доступ к соответствующей информации, «право на забвение» не должно применяться.

Следует также отметить неоднородность европейской судебной практики по вопросу связи «права на забвение» с основными правами человека или только с персональными данными. Ввиду этого необходимо рассмотреть два решения, вынесенные Кассационным судом Бельгии и Кассационным судом Франции.

В 2016 г. Кассационный суд Бельгии рассмотрел дело бельгийской газеты, у которой имелся онлайн-архив опубликованных статей, доступный для бесплатного просмотра. Одна из статей касалась осуждения истца приговором по уголовному делу, который был вынесен несколько лет назад и по которому он уже был реабилитирован. Воспользовавшись «правом быть забытым», истец подал в суд на главного редактора газеты с просьбой об удалении или анонимизации его данных и о возмещении ущерба.

Главный редактор утверждал, что «право быть забытым» в данном случае не может превалировать над свободой выражения мнений. Суд постановил, что «цифровое архивирование старой статьи в печатных средствах массовой информации не исключается из сферы действия “права на забвение”». Фактически онлайн-архивирование рассматриваемых статей было эквивалентно распространению фактов из-за их бесплатной доступности в Интернете.

По мнению Суда, во-первых, доступность статей в неанонимизированной версии представляла собой непропорциональное нарушение права человека на частную жизнь по сравнению с преимуществом, полученным с точки зрения свободы выражения мнений. Во-вторых, ограничение свободы выражения мнений являлось законным, поскольку все требования п. 2 ст. 10 Европейской конвенции по правам человека (далее — ЕКПЧ)[20] были соблюдены[21].

Вслед за этим, всего через 15 дней, Кассационный суд Франции вынес решение, в котором пришел к противоположным выводам: «Требование об удалении архивированной информации с сайтов средств массовой информации превышает рамки ограничений свободы прессы»[22]. Кассационный суд Франции считает, что «право на забвение» не оправдывает таких мер вмешательства в законодательство о печати, которые были бы связаны с обязанностью органа прессы удалять или разыменовывать информацию. Действительно, по соображениям защиты свободы выражения мнений право на персональные данные устанавливает особые режимы для прессы и средств массовой информации, к которым после принятия *GDPR* добавляются архивные цели. В этом случае сложнее отстаивать «право на забвение», основанное исключительно на праве на охрану чести и достоинства.

Таким образом, европейское законодательство предусматривает более широкое толкование и применение «права на забвение», включая перечень исключительных оснований, по которым оно не применяется. Нельзя не обратить внимание на тот факт, что Европейский союз

[20] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, Nov. 4, 1950, 1950 ETS 5. https://www.echr.coe.int/documents/convention_eng.pdf

[21] Cour de cassation [Cass.] [supreme court for judicial matters], Apr. 29, 2016, No. C.15.0052.F https://juricaf.org/arret/BELGIQUE-COURDECASSATION-20160429-C150052F

[22] Cour de cassation [Cass.] [supreme court for judicial matters] Chambre civile 1, May 12, 2016, No. 15-17.729, https://www.legifrance.gouv.fr/juri/id/JURITEXT000032532166/

связывает «право на забвение» непосредственно с законодательством о персональных данных, в то время как российский законодатель лишь внес поправки в действующий Закон об информации, а связь с персональным данными пока что существует только на уровне судебной практики.

Принципиальным отличием является и то, что европейское законодательство не позволяет применять «право на забвение» в случаях, когда такая информация представляется необходимой для реализации права на свободу выражения мнений и распространения информации, для архивных и статических целей, в общественных, научных или исторических интересах. Еще в решении *Google Spain* Европейский союз выразил озабоченность по поводу свободы выражения мнений, в том числе постановил, что при определенных обстоятельствах (например, когда личные данные касаются публичного лица) право общественности на доступ к этой информации должно преобладать. В российском законодательстве данный тезис подтверждается ст. 7 Закона об информации, согласно которой к общедоступной информации относятся сведения и иная информация, доступ к которой не ограничен, и она может использоваться любыми лицами по их усмотрению при соблюдении установленных законами ограничений в отношении распространения такой информации.

Несмотря на то что в эпоху цифровых технологий человек должен обладать правом контролировать свою личную информацию, физические лица не имеют и не должны иметь абсолютного права контролировать доступ к сведениям, касающимся их самих. Сам факт того, что информация затрагивает какое-либо лицо, является недостаточным для того, чтобы у последнего было право собственности на нее (Brimblecombe & Phillipson, 2018). В частности, физические лица не должны обладать правом ограничивать доступ к сведениям о себе, которые были опубликованы третьими лицами, за исключением случаев, когда такая информация носит клеветнический характер и когда ее публикация не оправданна по другим причинам. Другими словами, данные о людях также могут «принадлежать» общественности, которая, следовательно, должна иметь к ним доступ. Например, информация о банкротстве физического лица касается не только его самого, но и его кредиторов и контрагентов. Позволяя отдельным лицам разыменовать определенные факты, связанные с их именем, законодатель предоставляет им возможность устранить искаженное представление о себе. Общественность должна быть в состоянии составить собственное объективное мнение, основываясь на всей информации, доступной в Интернете. В особенности это касается лиц, осуществляющих предпринимательскую и политическую деятельность.

Следует отметить, что «право на забвение» распространяется только на физических лиц. Однако необходимость удалять сведения может касаться в том числе и юридических лиц. Действительно, неточная, вводящая в заблуждение, ложная или даже клеветническая информация может нанести такой же вред юридическому лицу, как и физическому, однако данный аспект остается не урегулированным в действующем законодательстве.

Непонятным также остается вопрос о квалификации сведений, подлежащих удалению оператором поисковой системы, так как российское законодательство не содержит четких критериев оценки неактуальной, утратившей значение для заявителя в силу последующих событий или действий заявителя информации. Отсутствие подобных критериев может послужить основанием для отказа в удалении сведений. Как следствие, возникнет неопределенность в практике применения «права на забвение».

«Право быть забытым» остается расплывчатым по ряду причин. Во-первых, до сих пор отсутствует законодательное определение баланса между «правом на забвение», с одной

стороны, и свободой выражения мнений, свободой доступа к информации — с другой. Во-вторых, «право на забвение» относится только к выдаче ссылок поисковых систем, в то время как информация на исходных сайтах по-прежнему остается. Очевидной причиной является фактическое преимущество права на свободу выражения мнений и свободный доступ к информации.

Право на забвение: новое право человека?

Как утверждает французский юрист Пьер Кайзер, «забвение является важнейшей ценностью, оно связано с самой природой человека, и отказ от права на забвение вызывает угрызения совести у человека, у которого нет другого будущего, кроме его прошлого, которое стоит перед ним как стена, закрывающая выход» (Kayser, 1984).

В связи с отсутствием законодательного закрепления термина «право на забвение» некоторыми исследователями высказывается мнение о том, что его можно рассматривать как часть права человека на защиту частной жизни, чести и доброго имени. Однако ввиду повсеместного использования Интернета и поисковых систем полагаем, что данное право следует определять как самостоятельное правовое явление, нуждающееся в отдельном закреплении. Практика международных судов и некоторых европейских государств свидетельствует о том, что определенная тенденция в этом направлении уже существует.

В 2021 г. был сделан еще один важнейший шаг к фактическому признанию «права на забвение» в качестве неотъемлемого права человека. Так, Европейский суд по правам человека (далее — ЕСПЧ) вынес решение о том, что приказ, требующий от издателя анонимизировать историческую статью в онлайн-архиве, не нарушает право издателя на свободу выражения мнений в соответствии со ст. 10 ЕКПЧ.

Верховный суд Бельгии обязал редактора газеты *"Le Soir"* анонимизировать статью в Интернете, в которой было указано имя мужчины, виновного в смертельном дорожно-транспортном происшествии. Требование об анонимизации было основано на «праве на забвение», а также на том факте, что осужденный уже был реабилитирован по данному делу.

В указанном споре ЕСПЧ взвесил право осужденного на защиту доброго имени и право редактора на свободу выражения мнений. Суд постановил, что требование об анонимизации виновного лица фактически нарушает право редактора на свободу выражения мнения. Однако, принимая во внимание необходимость защитить честь и достоинство осужденного, «наиболее справедливым способом обеспечить право осужденного на частную жизнь, не нарушая при этом непропорционально свободу выражения мнений редактора статьи, является анонимизация статьи».

О повышении значимости и актуальности признания «права на забвение» в качестве самостоятельной категории свидетельствует отход ЕСПЧ от ранее существовавшей в данном судебном органе практики. Так, в 2009 г. было вынесено постановление по делу *Financial Times Ltd. v. the United Kingdom*, в котором Суд придерживался противоположной логики. В частности, им указывалось на то, что свободе выражения мнения следует отдавать большее предпочтение, в связи с чем счел обоснованным установление сроков исковой давности по делам о диффамации в СМИ[23]. Безусловно, указанная логика противоречит основам применения «права на забвение», поскольку исключает возможность обращения к нему по прошествии некоторого времени.

[23] Financial Times Ltd. and Others v. the United Kingdom, No. 821/03. 2009 Eur. Ct. H.R. https://hudoc.echr.coe.int/fre?i=001-96157

Аналогичный подход был упомянут в постановлении ЕСПЧ 2018 г. по делу *M.L. and W.W. v. Germany*. Суть жалобы заключалась в том, что заявители требовали «права на забвение» и анонимизации опубликованных в СМИ сообщений о совершении ими преступления в 1991 г., в результате чего они были приговорены к пожизненному заключению. Суд поддержал позицию национальных органов о том, что право на доступ общественности к значимой информации имеет больший вес, чем право заявителей на неприкосновенность частной жизни по ст. 8 ЕКПЧ[24]. Как уже было указано, впоследствии вышеупомянутая позиция ЕСПЧ была пересмотрена в пользу права на неприкосновенность частной жизни. Главным в решении 2021 г. было заявление ЕСПЧ о том, что «право быть забытым» может быть включено в основные права человека согласно ст. 8 ЕКПЧ.

Данная практика является важнейшей предпосылкой и отправной точкой в законодательном включении «права на забвение» в перечень основных прав человека. Кроме того, заявители могут ссылаться на это решение для обоснования своих запросов на удаление информации из публикаций частных издателей.

До появления «права на забвение» в Законе об информации определенные предпосылки для защиты лица от распространения информации о нем против его воли содержались в гражданском законодательстве. В частности, ст. 150 ГК РФ предлагает расширенный подход к охране частной жизни, включая в данное понятие защиту от произвола не только со стороны государства, но и со стороны равнозначных субъектов (физических и юридических лиц), которые могут вторгнуться в частную жизнь и неправомерно использовать информацию о личности другого лица. Тем не менее согласно ст. 152 ГК РФ, посвященной защите чести, достоинства и деловой репутации, сведения могут быть признаны порочащими только в том случае, если они не соответствуют действительности. Согласно п. 2–5 ст. 152 Кодекса гражданин вправе потребовать удаления порочащей информации и публикации опровержения. Процедура опровержения более детально описывается в ст. 44 Закона РФ от 27 декабря 1991 г. № 2124-I «О средствах массовой информации».

Отсюда вытекает проблема следующего характера: согласно гражданскому законодательству удалению подлежит только та информация, которая не соответствует действительности. В таком случае ничто не препятствует распространению порочащих сведений, если они правдивы, что может серьезно сказаться на репутации и частной жизни лица. При определенных обстоятельствах гражданин может обратиться в правоохранительные органы на основании ст. 128.1 УК РФ, однако этот процесс может растянуться на годы, в течение которых порочащие сведения все еще будут доступны в сети Интернет.

Впрочем, именно с закреплением «права на забвение» указанная проблема была устранена: на основании ст. 10–10.3 Закона об информации граждане получили право требования удаления информации оператором поисковой сети, если она является недостоверной и неактуальной. Согласно п. 5 ст. 10.3 указанного акта оператор обязан прекратить выдачу ссылок на такую информацию в течение 10 дней с момента получения заявления. На наш взгляд, данная процедура существенно облегчает и ускоряет реализацию прав граждан.

В связи с высокой и постоянно возрастающей значимостью «права на забвение» в современных условиях полагаем, что его следует рассматривать не как составную часть права на неприкосновенность частной жизни, а как новое, самостоятельное право, поскольку, как уже было указано, в некоторых случаях они могут вступать в противоречие между собой. Вопрос о необходимости его закрепления на конституционном уровне остается открытым, поскольку сегодня

[24] M.L. and W.W. v. Germany, 2018 Eur. Ct. H.R. https://hudoc.echr.coe.int/eng?i=001-184438

это право существует на стыке гражданского и информационного права и не имеет четкой теоретической и практической базы. Тем не менее сегодня с уверенностью можно утверждать, что «право на забвение» как новый термин должно быть отражено в действующем законодательстве РФ.

Заключение

«Право на забвение» — концепция, возникшая в прошлом столетии и постепенно получившая закрепление в праве ЕС и национальном законодательстве отдельных государств, включая Россию. Анализ эволюции данного правового явления показал, что широкое признание оно получило относительно недавно — в начале 2010-х гг., после громкого дела *Google Spain*, рассмотренного Судом ЕС. В связи с этим теоретическая и практическая база реализации данного права имеет множество пробелов и недостатков и нуждается в незамедлительном совершенствовании. В частности, наибольшей критике подвергается факт, что в современной трактовке «право на забвение» представляет собой право требовать удаления информации только как ссылок в поисковых системах, но не в источнике первичной публикации. Таким образом, суть «права на забвение» заключается в ограничении доступа к информации, а не ее удалении (Carneroli, 2016).

Практика ЕС и отдельных европейских государств показывает, что «право на забвение» не имеет абсолютного характера. Во-первых, оно ограничивается по территориальному признаку: операторы поисковых систем, таких как *Google,* «Яндекс» и т.д., обязаны удалять ссылки только в рамках государства, гражданином которого является заявитель (в случае с гражданами ЕС — на всей территории ЕС). Во-вторых, в «праве на забвение» может быть отказано в тех случаях, когда информация представляет интерес для всего общества, а конституционные права граждан на доступ к ней и на свободу выражения мнений превалируют в силу общественной значимости сведений.

По итогам изучения «права на забвение» автором был выделен ряд актуальных проблем, касающихся правового закрепления данного явления. Во-первых, в некоторых случаях оно вступает в противоречие с правом на доступ к информации, а также ограничивает его, что не согласуется с ч. 4 ст. 29 Конституции РФ. Во-вторых, при определенных обстоятельствах «право на забвение» может рассматриваться как форма ограничения свободы выражения мнений в СМИ. В российском законодательстве сегодня не существует критериев, применимых для определения того, нарушает ли реализация «права на забвение» в конкретном случае конституционные права.

На настоящий момент самой большой проблемой, связанной с «правом на забвение» в контексте прав человека, является противоречие и препятствие свободе слова и доступа к информации. Если амнистия является актом, исходящим от власти, то «право на забвение» фактически реализуется частными компаниями по их усмотрению. На такие компании, как *Google* и «Яндекс», возложена ответственность за поиск баланса между интересами всего демократического общества и правами отдельного лица. Представляется, что частные компании не должны де-факто выполнять роль суда и обязаны по крайней мере руководствоваться законодательными принципами при принятии решений об удалении информации.

Для соблюдения баланса интересов в демократическом обществе необходимо, чтобы оценка применения «права на забвение» была в компетенции судов или независимых

органов по защите персональных данных. До тех пор пока не найдено юридическое и политическое решение этой проблемы, нужно представить поисковым системам свод правил и рекомендаций по реализации «права на забвение». С одной стороны, «право на забвение» должно гарантировать эффективность разыменования ошибочной или устаревшей информации, а с другой — оно не должно угрожать свободе доступа к информации для других пользователей.

Существуют опасения по поводу того, что поисковая система решит в одностороннем порядке удалить статьи, защищенные правом общественности на доступ к информации. Чтобы устранить эту проблему, следует ввести процедуру объективной оценки, в рамках которой заявитель, поисковая система и администратор сайта могли бы высказать свои суждения о необходимости оставления или удаления такой информации.

Кроме того, трудности, с которыми столкнулся Суд ЕС при рассмотрении вопроса об экстерриториальном действии «права быть забытым», демонстрируют необходимость разработки международного акта и режима охраны не только персональных данных, но и личной информации в целом, включая вопрос о применении «права на забвение» на мировом уровне. Представляется необходимой разработка единых международных стандартов применения «права на забвение» с экстерриториальными последствиями за пределами отдельных государств (Dechenaud, 2015). Принимая во внимание тот факт, что такие компании, как *Google,* осуществляют деятельность во всем мире, окончательно не решен вопрос об удалении ссылок со всех доменных имен поисковой системы. В отсутствие действующих международных стандартов, регулирующих обработку персональных данных, национальные юрисдикции могут повсеместно распространять свои стандарты конфиденциальности для гарантии полной защиты прав своих граждан (Susi, 2019).

Это указывает на необходимость закрепления понятия «право на забвение» в российском законодательстве для того, чтобы упрочнить тенденцию его формирования в качестве самостоятельного института. Так, предлагается внести поправки в Закон об информации путем замены ныне утратившей силу ст. 10.2 на новую статью с тем же номером под названием «Право на забвение». Следует указать следующее: ««Право на забвение» — это право требовать от оператора поисковых сетей немедленного удаления ссылок на персональные данные, которые подпадают под критерии, указанные в Законе». При этом основополагающими целями должны быть усиление контроля пользователей над их личной информацией и предоставление соответствующих гарантий, включая средства правовой защиты.

Несмотря на повсеместное применение «права на забвение», с ростом практики возрастают противоречивые случаи, которые требуют гармонизации. В связи с этим представляется необходимым внести уточняющие изменения в российское законодательство, регламентирующее порядок применения рассматриваемого права. В частности, предлагается дополнить п. 1 ст. 10.3 Закона об информации положением о том, что оператор поисковой системы вправе отказать в удовлетворении заявления об удалении ссылок в тех случаях, когда информация, содержащаяся в них, имеет общественную значимость или представляет общественный интерес. Под указанными категориями в таком случае следует понимать интерес общества в целом, а также заинтересованность широкой общественности в рамках политической, экономической и социальной ценности информации. Полагаем, что вышеописанный подход позволит упорядочить судебную практику по данному вопросу и привести ее к единообразию, а также снизить степень личного усмотрения операторов при принятии решения по заявлению.

Список литературы / References

1. Brimblecombe, F., & Phillipson, G. (2018). Regaining digital privacy? The new «right to be forgotten» and online expression. *Canadian journal of comparative and contemporary law*, *4*(1). 1–66.
2. Carneroli, S. (2016). *Le droit à l'oubli: Du devoir de mémoire au droit à l'oubli* [The right to be forgotten: From the duty of memory to the right to be forgotten]. Larcier.
3. Cofone, I.N. (Ed.). (2020). *The right to be forgotten: A Canadian and comparative perspective*. Routledge.
4. Dechenaud, D. (2015). *Le droit à l'oubli numérique: Données nominatives — approche comparée* [The right to digital oblivion: personal data — comparative approach]. Larcier.
5. Fabbrini, F., Celeste E. & Quinn, J. (Eds.). (2021). *Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty*. Hart Publishing.
6. Jones, M.L. (2016). *Ctrl + Z: The right to be forgotten*. NYU Press.
7. Kayser, P. (1984). *La protection de la vie privée: Protection du secret de la vie privée* [Protection of privacy: Protection of private life secrecy]. Presses Universitaires d'Aix Marseille.
8. Maietta, A. (2020). The right to be forgotten. *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito, 12*(2), 207–226. https://doi.org/10.4013/rechtd.2020.122.03
9. Mendel, T. (2018). *La liberté d'expression des parlements et des parlementaires: importance et périmètre de la protection: Guide à l'usage des parlementaires.* Union Interparlamentaire.
10. Susi, M. (2019). *Human rights, digital society and the law: A research companion*. Routledge.

Сведения об авторе:

Чуб Е. С. — старший юрист, ОАО «Автомир», Краснодар, Россия; аспирант кафедры международного частного и гражданского права им. С.Н. Лебедева, Московский государственный институт международных отношений (МГИМО-Университет) МИД России, Москва, Россия.
lenik21lenik@mail.ru

Information about the author:

Elena S. Chub — Senior Lawyer, OAO Avtomir, Krasnodar, Russia; Ph.D. Student, Department of Private International and Civil Law, MGIMO-University, Moscow, Russia.
lenik21lenik@mail.ru

https://doi.org/10.38044/2686-9136-2022-3-4-107-110

BOOK REVIEW

DIGITALIZATION OF ECONOMY: FROM NEO-KEYNESIANISM TO BLOCKCHAIN IN HEALTH CARE

Marina D. Simonova

MGIMO University
76, Prospect Vernadskogo, Moscow, Russia, 119454

Review of a book Deveraz, T., Leitão J., & Sarygulov A. (2021). *The Economics of Digital Transformation and Industrial Dynamics*. Springer. https://doi.org/10.1007/978-3-030-59959-1

Keywords digital economy, IT, economic theory, blockchain, energy, markets

For citation Simonova, M. D. (2022). Digitalization of economy: From Neo-Keynesianism to blockchain in health care. *Digital Law Journal, 3*(4), 107–110. https://doi.org/10.38044/2686-9136-2022-3-4-107-110

РЕЦЕНЗИЯ НА КНИГУ

ЦИФРОВИЗАЦИЯ ЭКОНОМИКИ: ОТ НЕОКЕЙНСИАНСТВА ДО БЛОКЧЕЙНА В ЗДРАВООХРАНЕНИИ

М.Д. Симонова

Московский государственный институт международных отношений (МГИМО-Университет) МИД России
119454, Россия, Москва, просп. Вернадского, 76

Рецензия на книгу Deveraz, T., Leitão J., & Sarygulov A. (2021). *The Economics of Digital Transformation and Industrial Dynamics*. Springer. https://doi.org/10.1007/978-3-030-59959-1

Ключевые слова цифровая экономика, IT, экономическая теория, блокчейн, энергетика, рынки

Для цитирования Симонова, М. Д. (2022). Цифровизация экономики: от неокейнсианства до блокчейна в здравоохранении. *Цифровое право, 3*(4), 107–110. https://doi.org/10.38044/2686-9136-2022-3-4-107-110

The book is published in the series *Studies on Entrepreneurship, Structural Change* and is devoted to the study of IT development and its impact on the digital transformation of the economy in modern conditions. The multinational team of authors comprises representatives of theoretical and applied scientific fields under the editorship of Tessaleno Devezas, João Leitão, and Askar Sarygulov.

Digital transformation and the rapid development of big data, ML, AI under present-day conditions concern all aspects of the development of economy and society. They alter the development of markets and industries, management techniques and decision-making methods. Many of the cutting-edge research reports are devoted to this.

In the monograph, the authors present several arguments for adjusting some of the tenets of economic theory, delve into the development of innovative IT solutions and their impact on the labor market, income, production, consumption and other economic factors. The book could be divided structurally into several generalized chapters. The author of the review conditionally divides it into three parts: theoretical, methodological and applied research. According to editors, 'It consists of providing innovative answers to still unexplored analysis topics, namely: (1) the socio-economic changes associated with the digital transformation of production systems; (2) the impacts of digital transformation on the sustainable functioning of socio-economic and environmental systems; (3) the adoption of intelligent/learning systems affecting the substitution of human labor force and smart digital management/security of cities, and (4) the type of materials and energy innovations leading to sustainable change'.

The book consists of 15 articles. The theoretical part thereof is aimed at drawing readers' attention to the contribution to academic science. It contributes to the research in the area.

Having conducted research with the use of mathematical apparatus under the headline "Social and Economic Consequences of Large-scale Digitization and Robotization of the Modern Economy", Askar Akaev, Andrey Rudskoy, and Tessaleno Deveza expect such labor market risks as a change in the employment structure, a dramatic decline in middle class bringing it on the verge of extinction, higher wages and falling incomes by 2050.

In research work headlined "Revisited Economic Theory or How to Describe the Processes of Disequilibrium and Instability of Modern Economic Systems" Askar Akaev and Viktor Sadovnichi devised nonlinear mathematical models, that accurately describe the Schumpeter-Kondratiev theory. These models can be used to calculate both long-term projected trajectories of the economic growth and cyclical fluctuations. The research reveals that the share of digital economy will grow. Developing the Keynes-Minsky theory, the authors propose to adjust the policy of public administration and make management of capital markets, which are effectively unstable, the focal point of central bankers.

Amid growing income disparity, the authors of the research article "Technological Development: Models of Economic Growth and Distribution of Income" Askar Akaev, Askar Sarygulov, and Valentin Sokolov make use of mathematical modeling and propose a modified neoclassical model of economic growth, which takes into account new empirical patterns. The authors prove that if state institutions do not interfere with existing trends, the rise in inequality will persist, since there are no endogenous economic mechanisms that could limit this process.

An empirical study of data on the US economy in the work "Breakthrough Technologies and Labor Market Transformation: How It Works and Some Evidence from the Economies of Developed Countries" by Elena Gorbashko, Irina Golovtsova, Dmitry Desyatko, and Viktorya Rapgof shows that job cuts in the industrial sector and job gains in the service sector are a long-term and sustainable trend. These structural transformation processes are not the result of market mechanisms alone.

State programs are needed to develop and finance personnel training and retraining to mitigate the consequences of profound structural changes in the labor market.

Askar Akaev, Andrey Rudskoy, and Tessaleno Devezas in the article "Technological Substitution of Jobs in the Digital Economy and Shift in Labor Demand Towards Advanced Qualifications" conduct mathematical modeling to identify the distribution of labor resources by skill level, as well as the distribution of the probability curve of technological displacement of labour depending on the skill level. This made it possible to calculate the actual share of low-, medium- and highly skilled workers before and after the digital transformation of the economy. The study shows that the optimum wage growth of highly skilled workers should be 7% per annum and double that in 10 years.

Recent changes in oil prices in 2021 have revived interest in oil shocks that affect international stock markets and are examined in the research paper "Oil Shocks and Stock Market Performance: Evidence from the Euro Zone and the USA". The authors Joao Leitao and Joaquim Ferreira calculate a VAR structural model to assess the impact of BRENT and WTI crude oil prices on the values of the Dow Jones, DAX, CAC, Athens Composite and PSI20 stock indices.

Maksim Balashov, Anton Kiselev, and Alena Kuryleva as part of the study "Reinforcement Learning Approach for Dynamic Pricing" try to solve the problem of dynamic pricing by maximizing profits from the sale of a specific product for automatic gas stations. To address this issue, the authors deem it appropriate to use machine learning methods that adapt to the environment, one of which being reinforcement learning (RL).

Examining the problem of creating the concept of cyber-physical systems in the research "Convergent Evolution of IT Security Paradigm: From Access Control to Cyber-Defense", Dmitry Zegzhda suggests we understand the security of cyber-physical systems as maintaining the stable functioning of a cyber-physical system, taking into account the targeted detrimental impact on its information components. The article describes the transition process from access control to cybersecurity for the full protection of cyber-physical systems.

Continuing the topic of cyber threats in the work "AI Methods for Neutralizing Cyber Threats at Unmanned Vehicular Ecosystem of Smart City", the authors Maxim Kalinin, Vasiliy Krundyshev, and Dmitry Zegzhda suggest using new AI methods (swarm algorithms and neural networks) to forestall cyber threats in V2X digital infrastructures and the results of experiments obtained using supercomputer modeling in intelligent environments such as IoT, IIoT, WSN, m2m networks.

Elaborating on cybersecurity in the research paper "Cybersecurity and Control Sustainability in Digital Economy and Advanced Production" Dmitry Zegzhda, Evgeny Pavlenko, and Anna Shtyrkina prove that an important feature of modern digital systems is the priority of ensuring the correct operation of the entire system, rather than the security of its individual components. The proposed approach is aimed at ensuring cybersecurity and cyberstability based on self-adaptation of the system to operating conditions.

In the article "Blockchain for Cybersecurity of Government E-Services: Decentralized Architecture Benefits and Challenges" Alexey Busygin and Artem Konoplev dissect the issue of different approaches to the creation of public e-services. The study reveals financial, operational and security-related advantages of the decentralized approach compared to the centralized one and identifies the pivotal problems of cybersecurity. The authors propose to use blockchain technologies in order to solve the problems in question.

The topic of energy problems is presented in the book at both sectoral and microeconomic levels. Yuri Nurulin, Inga Skvortsova, and Elena Vinogradova in the article "Green Energy Markets: Current Gaps and Development Perspectives in the Russian Federation" consider this pressing issue for

modern Russia in terms of the Doing Business rating. The authors carried out a comparative analysis of electric networks and their capabilities in the world and Russian economy. This study also examines the Smart Grid concept with a view to finding a way to ramp up network capacity.

In the article "Energy Efficiency in Urban Districts: Case from Polytechnic University" Yuri Nurulin, Vitaliy Sergeev, Inga Skvortsova, and Olga Kaltchenko consider an Energy Improvement District and as a real estate object in which energy efficiency measures are taken. This example can be replicated when it comes to private, state and regional real estate objects, which is important for stakeholders of territorial entities of St. Petersburg.

The article "An Architectural Approach to Managing the Digital Transformation of a Medical Organization" by Igor Ilin, Oksana Iliashenko, and Victoria Iliashenko revolves around the development of a medical organization's business model in the context of digitalization. The authors propose to use the architectural model of the upper level to implement new IT technologies and enhance the efficiency of health departments and in order to adapt the existing digital services in such departments.

Identifying the features of the development of commodity markets in the study headlined "Aluminum Production and Aviation: An Interesting Case of an Interwoven Rebound Effect in a Digital Transforming World" Tessaleno Devezas and Hugo Ruão analyze the dynamics of production and consumption of resources, including aluminum over the past 30 years. Econometric instruments are widely used to identify the impact of various factors (the Chinese market, ecology, scrap metal production, etc.) on aluminum consumption in space, aerospace and other industries. Resorting to forecast models for the period up to 2050, the authors conclude that under the influence of digitalization the amount of aluminum processed from scrap will suffice to produce aircraft.

Therefore, the book under review *The Economics of Digital Transformation and Industrial Dynamics* is a fundamental academic work. Even though it lacks a distinct structure, the general purpose of this book is to solve the problems inherent in IT development, as well as to implement information technologies at macro, meso and micro levels, given the call for expanding the foundations of economic theory. The book also sheds light on the quite relevant problem of the need to restructure enterprises and markets of goods and services in the context of digitalization tools, e-services, and IT on the whole. Such tools are being developed and improved in general. They have a practical meaning, for instance, in the energy sector and the healthcare system.

Information about the author:

Marina D. Simonova — Dr. Sci. in Economics, Professor, Accounting, Statistics and Auditing Department, MGIMO-University, Moscow, Russia.
m.simonova@inno.mgimo.ru
ORCID: https://orcid.org/0000-0003-2650-9932

Сведения об авторе:

Симонова М. Д. — доктор экономических наук, профессор кафедры учета, статистики и аудита, Московский государственный институт международных отношений (МГИМО-Университет) МИД России, Москва, Россия.
m.simonova@inno.mgimo.ru
ORCID: https://orcid.org/0000-0003-2650-9932